Dinion IP - NWC-0455

Security Systems

EN

Installation Manual
IP Camera

BOSCH

Copyright

This user guide is the intellectual property of Bosch Security Systems and is protected by copyright. All rights reserved. No part of this document may be reproduced or transmitted for any purpose, by whatever means, electronic or mechanical, without the express written permission of Bosch Security Systems.

Release: May 2006 (Software version 2.0)

© Copyright 2006 Bosch Security Systems

Note

This user guide has been compiled with great care and the information it contains has been thoroughly verified. The text was complete and correct at the time of printing. The ongoing development of the products may mean that the content of the user guide can change without notice. Bosch Security Systems accepts no liability for damage resulting directly or indirectly from faults, incompleteness or discrepancies between the user guide and the product described.

Trademarks

All hardware and software product names used in this document are likely to be registered trademarks and must be treated accordingly.

Contents

Important Safeguards vii
FCC Information viii

1. INTRODUCTION 11
Type number overview 12
Unpacking 12
System requirements 12
Overview of functions 13
Wide dynamic range 14
Power-over-Ethernet 14
Receiver 14
Video encoding 14
Tri Streaming 14
Recording 14
Multicast 14
Configuration 15
Tampering recognition and motion detectors 15
Snapshots 15
Backup 15

2. CONNECTIONS 16
Power 16
Network (and power) 16
Video service monitor 17
Alarm connector 17
Lens mounting 17
Mounting the camera 18

3. QUICK SET-UP 20
Back focus adjustment 20
Accessing and navigating quick set-up menu 21
How to use the navigation keys 21
Install menu 22
Install lens wizard submenu 22
Install IP address submenu 23
Defaults 24

4. NETWORK CONNECTION 25
System requirements (see page 12 for more detailed requirements) 25
Establishing the connection 25

5. OPERATION VIA THE BROWSER 27
Livepage 27
Image selection 27
Digital I/O 28
System log / Event log 28
Saving snapshots 28
Recording video sequences 28
Running recording program 29
Recordings page 29
Selecting recordings 30
Controlling playback 31

6. CONFIGURATION VIA THE BROWSER 33
Settings 33
General Settings 35
Camera identification 35
Password protection 36
Language selection 37
Date and time 37
Time server 38
Display Settings 38
Display stamping 38
Encoder Settings 39
Selecting an encoder profile 40
Changing profiles 41
JPEG posting 44
Camera settings 45
ALC 46
Enhance 47
Color 47
Installer options 48
Recording 49
Type 49
Storage information 49

iSCSI settings 50
Scan iSCSI IP address 51
iSCSI LUN map 51
Target IP address 51
Target name 51
Target LUN 52
Target password 52
Initiator name 52
Initiator extension 52
Decoupling the drive used 52
Storage information 52
Partitioning 53
Creating a partition 53
Saving changes 55
Editing a partition 55
Deleting partitions 56
Recording scheduler 57
Activating a partition for recording 57
Continuous recording 58
Recording status 58
Alarm recording 59
Properties 60
Alarm Settings *63*
Alarm in 63
Alarm connections 63
Video content analysis 65
Analysis 65
Analysis type 66
Motion detector 66
Sensitivity 66
Tamper detection 67
Alarm e-mail 70
Send alarm e-mail 70
Mail server IP address 70
Layout 70
Attach JPEG from camera 71
Destination address 71
Sender name 71

Send e-mail for testing 71
Relay Settings *71*
Alarm out 72
Service Settings *72*
Network 73
Multicasting 74
Version information 76
Livepage configuration 76
Licenses 79
Firmware and configuration upload 79
Function test 81

7. CONNECTIONS BETWEEN VIDEO SERVERS 82
Installation 82
Establishing the connection 82
Connect on alarm 82
Connecting with a Web browser 83
Closing the connection 83

8. OPERATION WITH DECODER SOFTWARE 84

9. MAINTENANCE 85
Testing the network connection 85
Repairs 85
Transfer and disposal 85

10. TROUBLESHOOTING 86

11. SPECIFICATIONS 88
Dimensions 89

12. ACCESSORIES 90
Recommended lenses 90
Power transformers 90

13. GLOSSARY 91

SAFETY PRECAUTIONS

Danger

The lightning flash with arrowhead symbol, within an equilateral triangle, is intended to alert the user to the presence of uninsulated “dangerous voltage” within the product's enclosure that may be of sufficient magnitude to constitute a risk to persons.

Warning

The exclamation mark within an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

Important Safeguards

1. Read these instructions.
2. Keep these instructions.
3. Comply with all warnings.
4. Follow all instructions.
5. Do not use this equipment near water.
6. Clean only with dry cloth.
7. Do not block any ventilation openings. Install in accordance with the manufacturer’s instructions.
8. Do not install near any heat sources such as radiators, heat registers, stoves, or other equipment (including amplifiers) that produce heat.
9. Do not defeat the safety purpose of the polarized or grounding-type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. Both the wide blade and the third prong are provided for your safety. If the supplied plug does not fit into your outlet, consult an electrician for advice.
10. Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the equipment.
11. Only use attachments/accessories specified by the manufacturer.

12. Unplug this equipment during lightning storms or when unused for long periods of time.
13. Refer all servicing to qualified service personnel. Servicing is required when the equipment has been damaged in any way, such as when power supply cord or plug is damaged, liquid has been spilled or objects have fallen into the equipment, the equipment has been exposed to rain or moisture, does not operate normally, or has been dropped.
14. An all-pole mains switch with a contact separation of at least 3mm in each pole shall be incorporated in the electrical installation of the building.

Warning

To reduce the risk of electric shock, do not remove covers. No user-serviceable parts inside. Refer servicing to qualified service personnel.

Warning

To reduce the risk of fire or electric shock, this apparatus should not be exposed to rain or moisture and objects filled with liquids, such as vases, should not be placed on this apparatus.

FCC Information

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

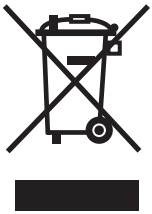
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

Note

Any change or modification of the equipment not expressly approved by Bosch could void the user's authority to operate the equipment.

For additional information or to speak to a representative, please contact the Bosch Security Systems location nearest to you or visit our web site at www.boschsecuritysystems.com

Only for EU countries



Do not dispose of electric tools together with household waste material!

In observance of European Directive 2002/96/EC on waste electrical and electronic equipment and its implementation in accordance with national law, electric tools that have reached the end of their life must be collected separately and returned to an environmentally compatible recycling facility.

Caution

The power supply unit must comply with EN/UL 60950 or equivalent safety standard. The power supply unit must be a SELV (Safety Extra Low Voltage) source with single fault protection. IEEE802.3af compliant power sources are SELV devices by default.

1 Introduction

The Dinion IP camera is a high-performance smart surveillance color camera. It incorporates advanced digital signal processing for outstanding picture performance. The camera operates as a network video server and transmits video and control signals over data networks such as Ethernet LANs and the Internet.

The Dinion IP camera is easy to install and ready to use, and offers the best solution for demanding scene conditions. Features include:

- NightSense™ extends the low-light performance of the camera
- Enhanced video motion detection
- Video and data transmission over IP data networks
- Tri Streaming function for simultaneous encoding with three individually definable profiles
- Multicast function for simultaneous picture transmission to multiple receivers
- One analog composite video output CVBS (PAL/NTSC)
- Video encoding using international MPEG-4 standard
- Integrated Ethernet interface (10/100 Base-T)
- Remote control of all built-in functions via TCP/IP
- Password protection to prevent unauthorized connection or configuration changes
- Relay input for external sensor (such as door contacts)
- Event-driven, automatic connection (for example at switch-on and for alarms)
- Fast, convenient configuration using the integrated Web server and a browser
- Firmware update through flash memory
- Convenient upload and download of configuration data

Type number overview

Type number	NWC-0455-10P	NWC-0455-20P
Standard	50 Hz	60 Hz
Supply voltage	24 VAC or 12 VDC (use class 2 power supply) or PoE (IEEE 802.3af)	
CCD type	1/3"	

Unpacking

Unpack carefully and handle the equipment with care. The packaging contains:

- Dinion^{XF} IP camera
- CS to C lens mount adapter
- CCD protection cap
- Spare lens connector (male)
- CD ROM
  - Quick Installation Guide
  - Manual
  - Configuration Manager
  - MPEG ActiveX control
  - MPEG viewer
  - Adobe Acrobat Reader
- Quick install instructions

Note
If equipment appears to have been damaged during shipment, repack it in the original packaging and notify the shipping agent or supplier.

System requirements

- Computer with Windows 2000/XP operating system, network access and Microsoft Internet Explorer web browser version 6.0 or later
  or

- Computer with Windows 2000/XP operating system, network access and reception software, for example VIDOS or DIBOS 8.0
  or
- MPEG-4 compatible hardware decoder from Bosch Security Systems (such as VIP XD) as a receiver and a connected video monitor

The minimum PC requirements are:

- Operating platform: A PC running Windows 2000 or Windows XP with IE6.0
- Processor: 1.8 GHz Pentium IV
- RAM memory: 256 MB
- Video system: 128 MB video memory, 1024x768 display with 24-bit color
- Network interface: 100-BaseT
- DirectX: 9.0b

Note
Make sure the graphics card is set to 16-bit or 32-bit color depth and that Microsoft Virtual Machine or Java Virtual Machine is installed on your PC. To play back live video images, an appropriate MPEG ActiveX must be installed on the computer. If necessary, install the required software and controls from the product CD provided. If you need further assistance, contact your PC system administrator.

Overview of functions

The camera incorporates a network video server. Its primary function is to encode video and control data for transmission over an IP network. With its MPEG-4 encoding it is ideally suited for IP communication and for remote access to digital video recorders and multiplexers. The use of existing networks means that integration with CCTV systems or local networks can be achieved quickly and easily. Video images from a single camera can be simultaneously received on several receivers.

Wide dynamic range

The digital signal is automatically processed in the camera to optimally capture the detail in both the high and low light areas of the scene simultaneously, maximizing the information visible in the picture.

Power-over-Ethernet

Power for the camera can be supplied via a Power-over-Ethernet (IEEE 802.3af) compliant network cable connection. With this configuration, only a single cable connection is required to view, power and control the camera.

Receiver

MPEG-4 compatible hardware decoders (for example VIP XD) can be used as a receiver. Computers with decoding software such as VIDOS or computers with the Microsoft Internet Explorer web browser installed can also be used as receivers.

Video encoding

The camera uses the MPEG-4 compression standard. Thanks to efficient encoding, the data rate remains low even with high image quality and can also be adapted to local conditions within wide limits.

Tri Streaming

Tri Streaming allows the incoming data stream to be encoded simultaneously according to three different, individually customized profiles. This creates two MPEG4 streams per camera that can serve different purposes, for example one for local recording and one optimized for transmission over the LAN, and an additional JPEG stream for use with a PDA for example.

Recording

The NWC-0495 can be used with an iSCSI server connected via the network to store long-term recordings.

Multicast

In suitably configured networks, the multicast function enables simultaneous, real time transmission to multiple receivers. The prerequisite for this is that the UDP and IGMP V2 protocols are implemented on the network.

Configuration

The camera can be configured using a browser on the local network (Intranet) or from the Internet. Similarly, firmware updates and rapid loading of device configurations are also possible. Configuration settings can be stored as files on a computer and copied from one camera to another.

Tampering recognition and motion detectors

The NWC-0495 offers a wide range of configuration options for alarm signaling in the event of tampering with the camera. An algorithm for detecting movement in the video image is also part of the scope of delivery and can optionally be extended to include special video analysis algorithms.

Snapshots

Individual video frames (snapshots) can be called up as JPEG images, stored on the hard drive or displayed in a separate browser window.

Backup

The browser application Livepage has an icon for saving the video images provided by the unit as a file on your computer's hard drive. Clicking this icon stores the video sequences and they can be replayed with the MPEG viewer from Bosch Security Systems included with the package.

Connections 2

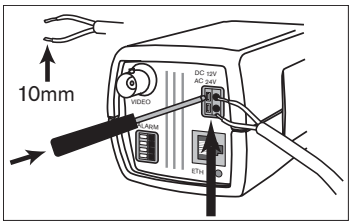
Power

Caution

Ensure that your power supply matches the rated voltage of your camera before installing.

Caution

Never supply power via the power connector when power is supplied via the Ethernet connection (PoE).

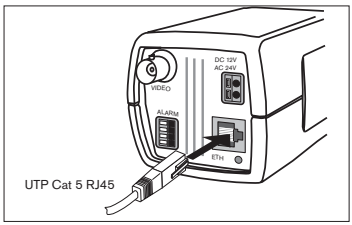


- use a class 2 power supply
- 24 VAC or 12 VDC
- push in the tabs to open the quick-connectors (these connections are not polarity sensitive).
- use AWG16 to 22 stranded wire or AWG16 to 26 solid wire; cut back 10mm (0.4") of insulation.

Network (and power)

Caution

Never supply power via the Ethernet connection (PoE) when power is supplied via the power connector.

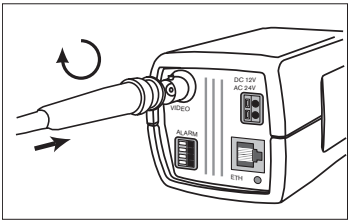


- connect the camera to a 10/100 Base-T network.
- use a shielded UTP Category 5 cable with RJ45 connectors.
- Power can be supplied to the camera via the Ethernet cable compliant with the Power-over-Ethernet (IEEE 802.3af) standard.

Note

The multicolored LED under the Ethernet connection indicates Power (red), IP connection (green) and IP traffic (green flashing). It can be disabled in the `Settings/Camera Settings/Installer options` menu.

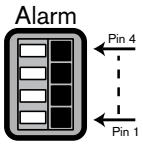
Video service monitor



- connect a service monitor to the composite video BNC connector to aid installation.
- a monitor connected close to the camera via this connection can also be used in parallel with remote PC viewing.

Alarm connector

Pin	Alarm socket
1	Ground
2	Alarm in
3	Relay out contact 1
4	Relay out contact 2



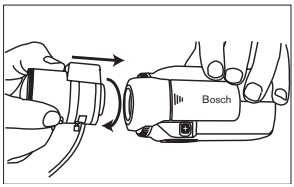
- Max. wire diameter AWG 22-28 for both stranded and solid.
- Default relay position n.o. (normally open), no alarm.
- Alarm output relay switching capability: Max voltage 30VAC or +40VDC. Max 0.5 A continuous, 10VA.
- Alarm in: TTL logic, +5V nominal, +40VDC max, DC coupled with 22kOhm pull-up to +3.3V.
- Alarm in: configurable as active low or active high.
- Max. 42V allowed between camera ground and each of the relay pins.

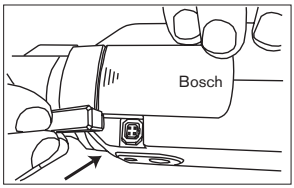
Lens mounting

The camera accepts CS-mount lenses with a lens protrusion of up to 5mm. C-mount lenses can be mounted using the lens adapter ring. DC-iris lenses are recommended for the best picture performance. The camera automatically detects the type of lens used and optimizes performance accordingly. A spare male lens connector is provided.

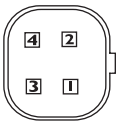
Caution

To avoid damaging the CCD sensor when using a C-mount lens, make sure the supplied lens adapter ring is mounted onto the camera before mounting the lens.
Lenses weighing more than 0.5 kg (1.1lbs) must be separately supported.





Pin	Video iris lens	DC iris lens
1	Supply (11.5V ±0.5, 50mA max.)	Damp -
2	Not used	Damp +
3	Video signal 1Vpp 1kOhm	Drive +
4	Ground	Drive -

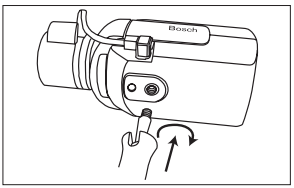


Note

If a short circuit is detected on the lens connector, the on-screen display (OSD) failure message LENS SHORT CIRCUIT is shown. The lens circuit is automatically disabled to avoid internal damage. Remove the lens connector and check the pin connections.

Mounting the camera

The camera can be mounted from the top or bottom. The bottom mounting is isolated from ground. With outdoor scenes, a DC-iris lens is recommended.



Caution

Do not point the camera/lens into direct sunlight.
Do not obstruct the free flow of air around the camera.

Note

The camera becomes quite warm when operating; this is normal.
However, you should take this into account when touching the camera.

3 Quick set-up

The Dinion IP camera normally provides an optimal picture without the need for further adjustments. Configuration of the camera is carried out remotely via the network using a web browser. However, the camera also has an Installer menu in which basic installation settings (lens wizard, IP address) can be accessed. To view this menu connect a monitor to the composite video output of the camera.

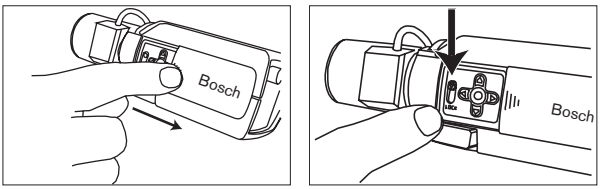
Back focus adjustment

To optimize picture sharpness in both bright and low-level lighting, adjust the back focus. Use the camera's unique Lens Wizard. This ensures that the object of interest always remains in focus even when focusing at the maximum lens opening.

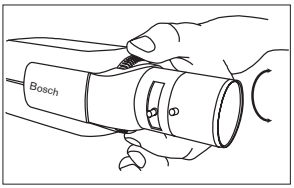
- When back focusing vari-focus lenses, adjust to obtain a sharp picture in both wide-angle and tele positions for both far and near focus.
- When back focusing zoom lenses, ensure the object of interest remains in focus throughout the entire zoom range of the lens.

To adjust back focus:

1. Open the slide door at the side of the camera
2. Unlock the back focus locking button.



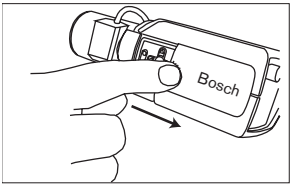
3. Turn the back focus adjustment as required.

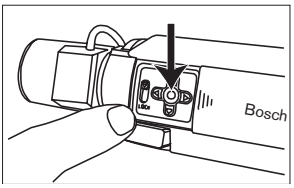


4. Lock the back focus locking button.

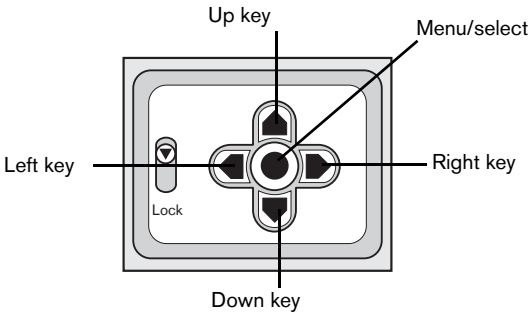
Accessing and navigating quick set-up menu

Five keys, located behind the side panel, are used for navigating through the quick set-up menu. To access the set-up menus, press the menu/select key (center). The main menu appears on the monitor.





How to use the navigation keys



- Press the menu/select key to access the menus or to move to the next or previous menu.
- Press the menu/select key for approximately 1.5 seconds to open the Installer menu.
- Use the up or down keys to scroll up or down through a menu.

- Use the left or right keys to move through options or to set parameters.
- When in a menu, quickly pressing the menu/select key twice restores the selected item to its factory default.
- To close all menus at once from any menu, select the Exit item and hold down the menu/select key until the menu display disappears.

Install menu

Function	Selection	Description
Lens Wizard	Select submenu	Select to optimize camera lens combination
Network	Select submenu	Select to set the network IP address for the camera (default address is 192.168.0.1)
Exit		Exit the menu

Install lens wizard submenu

Function	Selection	Description
Lens Type	AUTO, MANUAL, DCIRIS, VIDEO	In AUTO mode the camera auto detects the type of lens used or force the camera into a mode.
Detected		If the LENS TYPE detection is in AUTO, the detected lens type is shown.
Set Back Focus Now		Select to force lens to its maximum opening. After focusing the lens the object of interest remains in focus in bright and low light conditions.
Set LVL		(Video iris lenses only). The level detector indicator must be set to the center by adjusting the level potentiometer on the lens, to obtain the best picture performance.
Exit		Return to the INSTALL menu

Adjustment procedure DC-iris Lens

1. Unlock the back focus locking button.
2. Access the `Lens Wizard` menu.
3. `Set Back Focus Now` is highlighted in the menu.
4. Turn the back focus adjustment as required.
5. Lock the back focus locking button.
6. Exit the menu.

Adjustment procedure Manual-iris Lens

1. Unlock the back focus locking button.
2. Adjust the lens to the maximum lens opening.
3. Turn the back focus adjustment as required.
4. Lock the back focus locking button.

Adjustment procedure Video-iris Lens

1. Unlock the back focus locking button.
2. Access the `Lens Wizard` menu.
3. `Set Back Focus Now` is highlighted in the menu.
4. Turn the back focus adjustment as required.
5. Lock the back focus locking button.
6. Select `Set LVL` in the menu; the `Level` bar appears.
7. Point the camera at the scene it will be mostly viewing.
8. Adjust the level potentiometer located on the lens until the `Level` bar is in the central position.
9. Exit the menu.

Note

The best performance with video iris lenses is obtained when the peak/average potentiometer of the lens matches the peak/average balance configuration setting.

Install IP address submenu

To operate the camera in your network, a network-valid IP address must be assigned. The factory default IP address is 192.168.0.1

Function	Selection	Description
IP Address		Enter an IP address for the camera. Use LEFT/RIGHT to change position in the address, use UP/DOWN to select the digit. Use SELECT to exit the address edit screen.
Subnet Mask		Enter the Subnet mask (default 255.255.255.0)
Gateway		Enter a Gateway address.
Exit		Return to the Install menu

Note

The new IP address, subnet mask and gateway address are set after you leave the menu. The camera reboots internally and the new values are set after a few seconds.

Defaults

To restore all parameters (including IP address) to the factory defaults, press and hold the Up navigation key for at least 10 seconds and then confirm. Allow a few seconds for the camera to optimize the picture after a mode reset.

Note

Restoring the factory defaults may result in the loss of the IP connection. If this occurs, change the IP address of your browser to the factory default value. Only restore the factory defaults when it is absolutely necessary.

4 Network connection

A computer with Microsoft Internet Explorer can be used to receive live images from the camera, control cameras and replay sequences stored on the local hard drive. The camera is configured over the network using the browser or via the Configuration Manager (supplied with the product). The configuration options using the menu system of the camera itself are limited to setting up the lens and network.

Note
The camera can also be connected to DIBOS 8.0, VIDOS and BVMS video management systems as well as third party video management systems.

System requirements (see page 12 for more detailed requirements)

- Microsoft Internet Explorer version 6.0 or higher
- Monitor resolution 1024 × 768 pixels
- Intranet or Internet network access

To play back live video images, an appropriate MPEG ActiveX must be installed on the computer. If necessary, the required software and controls can be installed from the product CD provided.

– Insert the CD into the CD-ROM drive of the computer. If the CD does not start automatically, open the root directory of the CD in Windows Explorer and double click MPEGAx.exe.
– Follow the on-screen instructions.

Establishing the connection

The camera must be assigned a valid IP address to operate on your network. The default address pre-set at the factory is 192.168.0.1

– Start the Web browser.
– Enter the IP address of the camera as the URL.

Password protection in camera

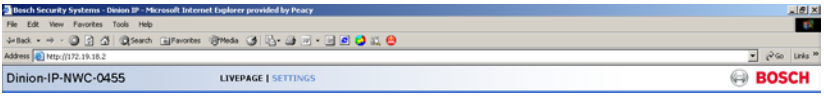
If the camera is password-protected, a message to enter the password appears.

Note

A camera offers you the option of limiting access across various authorization levels.

– Enter the user name and the associated password in the appropriate fields.
– Click OK. If the password is correct, the desired page is displayed.

After a short time when the connection is established, the Livepage with the video image appears. In the application title bar the Livepage selection is used to operate the camera; the Settings selection is used to configure the camera and the application interface.



Note

If the connection is not established, the maximum number of possible connections may already have been reached. The maximum number of connections depends on the device and network configuration.

5 Operation via the browser

Livepage

After the connection is established, the Livepage is initially displayed. It shows the live video image on the right of the browser window. Depending on the configuration, various text overlays may be visible on the live video image. Other information may also be shown next to the live video image on the Livepage. The display depends on the settings on the Livepage configuration page.

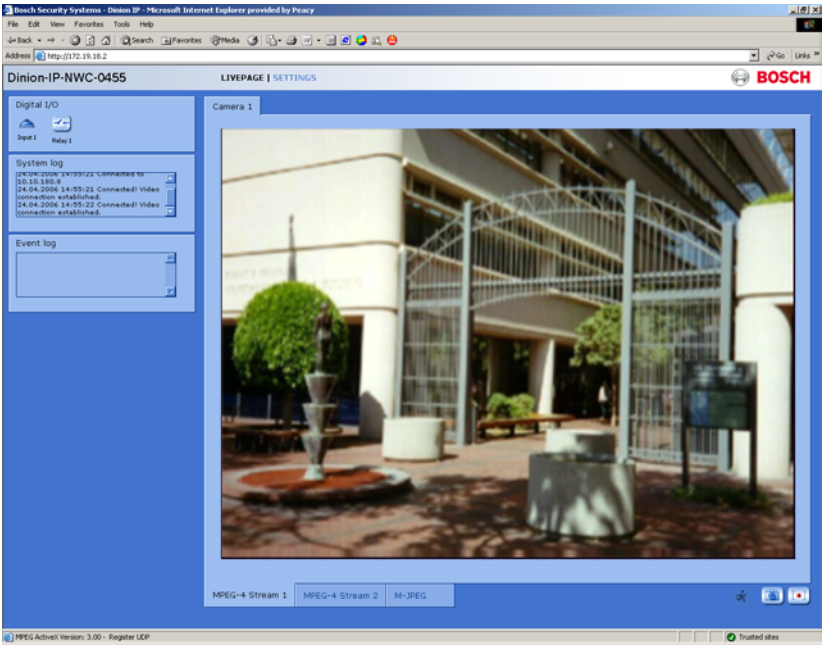


Image selection

You can view the image on a full screen.

– Click on one of the MPEG-4 Stream 1, MPEG-4 Stream 2 or M-JPEG tabs below the video image to switch between the different displays for the camera image.

Digital I/O

Depending on the configuration of the unit, the alarm input and the relay output are displayed next to the camera image. The alarm symbol is for information and indicates the input status of the alarm input: Active 1 = Symbol is green, Active 0 = Symbol not lit. The relay on the camera allows you to operate a device (for example a light or a door opener).

– To operate, click the relay symbol next to the video image. The symbol is red when the relay is activated.

System log / Event log

System log
Video connection established.
Jun 16, 2005 9:39:23 AM Connected!
Video connection established.
Jun 16, 2005 9:41:17 AM Snapshot camera 1:
c:\16_06_2005_09_41_16_cam1.jpg
Event log
alarm 1 cleared.
Jun 16, 2005 9:39:41 AM Motion alarm 1 detected.
Jun 16, 2005 9:39:48 AM Motion alarm 1 cleared.

The System log field contains information about the operating status of the camera and the connection. These messages can be saved automatically in a file. Events such as the triggering or end of alarms are shown in the Event log field. These messages can be saved automatically in a file.

Saving snapshots

Individual images from the video sequence that is currently being shown on the Livepage can be saved in JPEG format on the computer's hard drive.

– Click the camera icon to save single images.

– The image is saved at a resolution of 704 × 576/480 pixels (4CIF). The storage location depends on the configuration of the camera.

Recording video sequences

Sections of the video sequence that is currently being shown on the Livepage can be saved on the computer's hard drive. The sequences are recorded at the

resolution specified in the encoder configuration. The storage location depends on the configuration of the camera.

- Click the recording icon to record video sequences.
- Saving begins immediately. The red dot on the icon flashes to indicate that a recording is in progress.
- Click the symbol for recording video sequences again. Saving is terminated.

Installing MPEG viewer

You can play back saved video sequences using the MPEG viewer from Bosch Security Systems, which can be found on the software CD supplied.

Note
A corresponding MPEG ActiveX (located on the CD provided with the product) must be installed on the computer in order to play back saved video sequences using the MPEG viewer.

- Insert the CD into the CD-ROM drive of the computer. If the CD does not start automatically, open the CD in the Windows Explorer.
- Open the MPEG Viewer directory and copy the file MPEGViewer.exe to your computer's hard drive.
- If necessary, you can also start the MPEG viewer by double-clicking the file MPEGViewer.exe.

Running recording program

The hard drive icon below the camera images on the Livepage changes during an automatic recording to the RAM memory of a NWC-0495 or to an iSCSI storage device.

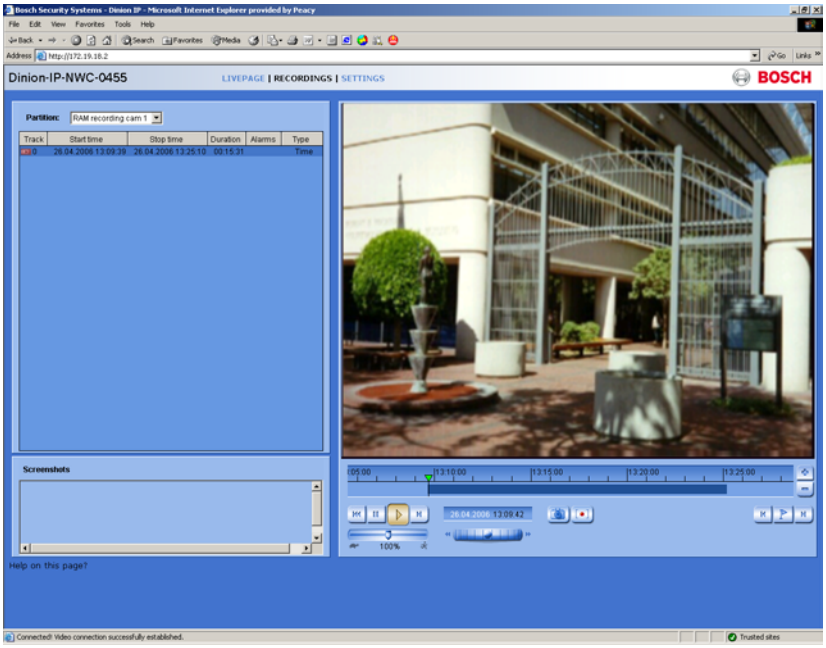
The icon lights up and displays a moving graphic to indicate a running recording. If no recording is taking place, a gray icon is displayed.

Recordings page

You can access the Recordings page for playing back recorded video sequences from the Livepage as well as from the Settings menu.

The Recordings link is only visible if a storage medium has been selected (see “Recording” on page 49).

- Click in the navigation bar in the upper section of the window on the link Recordings The playback page appears.



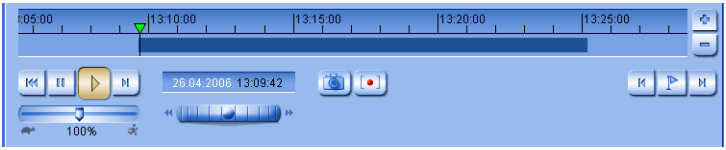
Selecting recordings

In the left section of the page, first select the partition whose recordings you want to view.

All sequences that are saved in the partition are displayed in the list. A running number (track) is assigned to each sequence. Start time and stop time, recording duration, number of alarms, and recording type are displayed.

- Click a partition name from the list to display the recordings for this partition.
- Click a list entry. The playback for the selected sequence starts immediately in the video window.

Controlling playback



You will see a time bar below the video image for quick orientation. If a particular sequence has been selected for playback by means of click, the selected sequence is highlighted. The associated time interval is displayed in the bar in blue. A green arrow above the bar indicates the position of the image currently being played back within the sequence.

The time bar offers various options for navigation in and between sequences.

- You can change the time interval displayed by moving the blue area to the left or right while holding down the mouse button.
- You can change the time interval displayed by clicking the plus or minus icons. The display can span a range from two months to a few seconds.
- You can select a different sequence for playback by clicking on the corresponding blue marking.
- If required, drag the green arrow to the point in time at which the playback should begin. Alternatively you can double-click directly in the blue time interval or in the timescale to jump to the position selected in this manner. The date and time display below the bar provides orientation to the second.

You can control playback by means of the buttons below the video image.
The buttons have the following functions:

Start playback

Pause playback

Jump to start of active video sequence or to previous sequence in the list

Jump to end of active video sequence or to next sequence in the list

You can use the slide control to control playback speed and fast forward/rewind: positioning in the middle indicates playback at recording speed, left indicates rewind, and right fast forward. The fast forward or rewind speed changes, depending on how far you move the slide control toward the runner icons.

You can continuously select playback speed by means of the speed regulator:

Red bars within the bluegray sequence fields indicate the points in time where alarms were triggered. Drag the green arrow to navigate to these points quickly.

In addition, you can set markers in the sequences, so-called bookmarks, and jump directly to these. These bookmarks are indicated as small yellow arrows above the time interval. Use the bookmarks as follows:

Jump to the previous bookmark

Set bookmark

Jump to the following bookmark

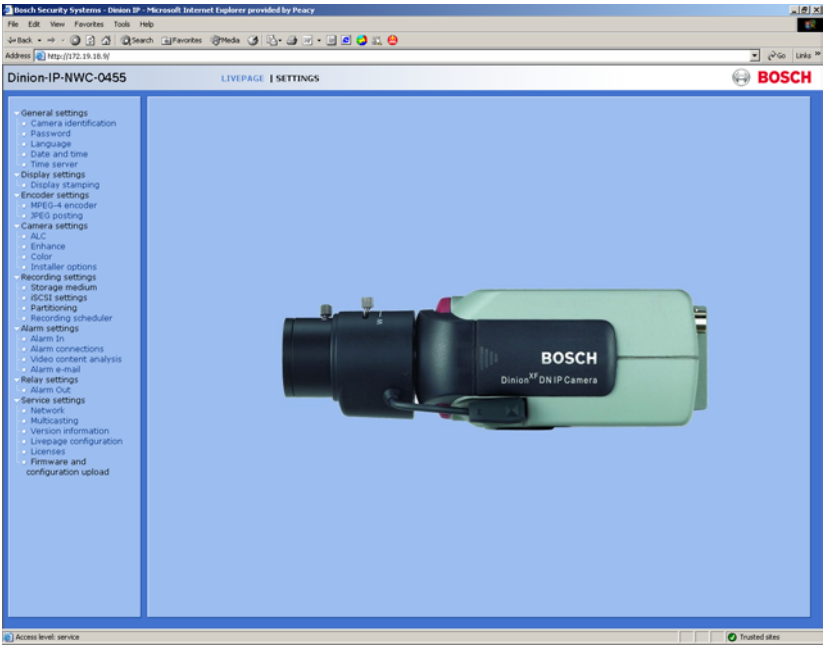
- Right-click a bookmark to delete it.

Note
Bookmarks are only valid while you are in the Recordings page; they are not saved with the sequences. As soon as you leave the page all bookmarks are deleted.

6 Configuration via the browser

Settings

When a connection is established, the Livepage is initially displayed. Click Settings in the application title bar to configure the camera and the application interface. A new page containing the configuration menu is opened.

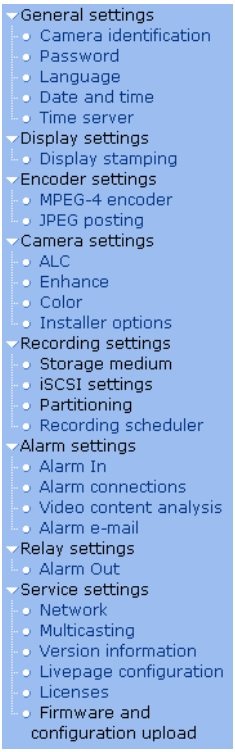


All settings are stored in the camera memory, and they are preserved even if the power is interrupted.

Configuration menu tree

The configuration menu tree allows all parameters of the camera to be configured. The configuration menu is recommended for expert users or system administrators. All unit parameters can be accessed in this mode. Changes that

influence the fundamental functioning of the unit (for example firmware updates) can only be made using the configuration menu.



You can view the current settings by opening one of the configuration pages.

– Click on one of the menu options on the left of the window. The associated sub-menu is opened.
– Click one of the links in the sub-menu. The corresponding page is opened.

The settings are changed by entering new values or by selecting a pre-defined value in a list field.

Saving changes

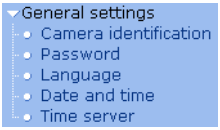
After making changes in a window, click the Set button to send the new settings to the unit and save them there.

Note

Save the changes made in each window by clicking Set. Clicking the Set button saves only the settings in the current window. Changes in any other fields are ignored.

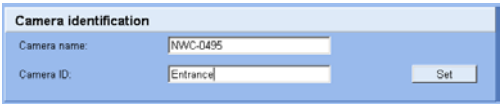
Click on the Settings link at the top of the window to close the window without saving the changes made.

General Settings



Various basic data for the camera can be set or selected here.

Camera identification



Camera name

The camera can be assigned a name to assist in identifying it. The name simplifies the management of multiple devices in more extensive systems, for example using the VIDOS software.

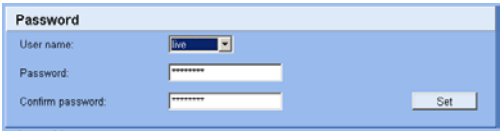
Note

The camera name is used for remote identification of a unit, in the event of an alarm for example. Enter a name that makes it as easy as possible to identify the location unambiguously.

Camera ID

Each camera should be assigned a unique identifier that can be entered here as an additional means of identification.

Password protection



A camera is generally protected by a password to prevent unauthorized access to the unit. You can use various authorization levels (User name:) to limit access.

Note

Proper password protection is only guaranteed if all higher authorization levels are also protected with a password. For example, if a live password is assigned, a service and a user password should also be set. When assigning passwords, you should always start from the highest authorization level.

User name

The camera recognizes three user names: service, user and live, which correspond to different authorization levels.

- The user name service represents the highest authorization level. After entering the corresponding password, you can use it to access all the functions of the camera and change all configuration settings.
- The user name user represents the middle authorization level. You can use it to operate the unit and also to control cameras, but you cannot change the configuration.
- The user name live represents the lowest authorization level. It can only be used to view the live video image and switch between the different live image displays.

Password

You can define and change a separate password for each user name if you are logged on as Service or if the unit is not protected by a password. Enter the password for the selected user name here.

Confirm password

Re-enter the new password to rule out typing mistakes.

Note

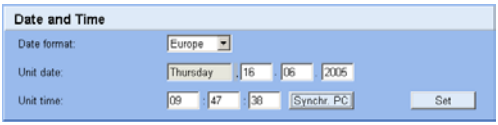
The new password is then saved by clicking the Set button. You should therefore click the Set button immediately after entering and confirming the password, even if you also want to assign a password to another user name.

Language selection

Website language

Select the language for the user interface here.

Date and time



Date format

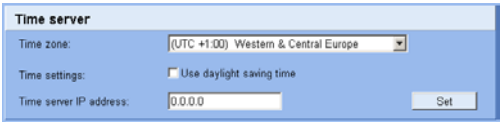
Choose the desired date format here
(Europe: DD.MM.YYYY; USA: MM.DD.YYYY; Japan: YYYY/MM/DD).

Unit date and time

If there are a number of devices operating in your system or network, it is important to synchronize their internal clocks. For example, it is only possible to carry out correct identification and evaluation of recordings occurring at the same time if all devices are operating on the same time.

- Enter the current date. Since the unit time is controlled by the internal clock, it is not necessary to enter the day of the week. This is added automatically.
- Enter the current time or click Synchr. PC to apply the system time from your computer to the camera.

Time server



The camera can receive the time signal from a time server using the time server protocol (RFC 868) and then use it to set the internal clock. The device calls up the time signal automatically every ten minutes.

Time zone

Select the time zone in which the system is located.

Time settings

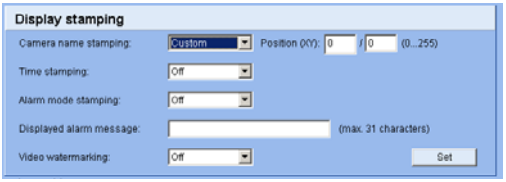
Select this during daylight savings time if the time change is to be taken into account. Deactivate the check box to switch to winter time.

Time server IP address

Enter the IP address of a time server working with the RFC 868 protocol.

Display Settings

Display stamping



Various overlays or stamps in the video image provide important supplementary information. These overlays can be enabled individually and arranged on the image in a clear manner.

Camera name stamping

This field sets the position of the camera name overlay. It can be displayed at the Top, at the Bottom or at a position of your choice using the Custom option. Or it can be set to Off if no overlay of this information is to be shown.

Time stamping

This field sets the position of the time and date overlay. It can be displayed at the Top, at the Bottom or at a position of your choice, which you have pre-defined using HyperTerminal, using the Custom option. Or it can be set to Off if no overlay of this information is to be shown.

Alarm mode stamping

Choose On if a text message should be overlaid in the event of an alarm. It can be displayed at a position of your choice using the Custom option. Or it can be set to Off if no overlay of this information is to be shown.

- Select the desired position from the lists.
- If you have selected the Custom option, additional fields are displayed to specify the exact position (Position (XY):).
- In the Position (XY): fields enter the values for the desired position.

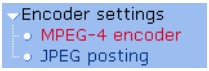
Displayed alarm message

Enter the message to be displayed for an alarm. It can contain up to 31 characters.

Video watermarking

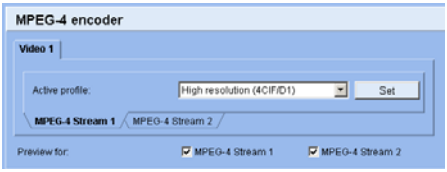
Choose On if the video images transmitted are to be watermarked. After activation, all images are marked with a small green rectangle. A red rectangle indicates that the sequence (live or saved) has been manipulated.

Encoder Settings



For encoding the video signal, you can select two profiles and change the presets for the profiles.

Selecting an encoder profile



You can adapt the MPEG-4 data transmission to the operating environment (for example network structure, bandwidth, data structures). To do this, the camera simultaneously generates two data streams (Dual Streaming), for which you can select different compression settings, for example one setting for transmissions to the Internet and one for LAN connections.

Pre-programmed profiles are available, which each give priority to different perspectives.

- Profile 1: Low bandwidth (CIF)
  High quality for low bandwidth connections, resolution 352 × 288/240 pixels
- Profile 2: Low delay (2/3 D1)
  High quality with low delay, resolution 464 × 576/480 pixels
- Profile 3: High resolution (4CIF/D1)
  High resolution for high bandwidth connections, resolution 704 × 576/480 pixels
- Profile 4: DSL
  For DSL connections at 500 kBit/s, resolution 352 × 288/240 pixels
- Profile 5: ISDN (2B)
  For ISDN connections via two B channels, resolution 352 × 288/240 pixels
- Profile 6: ISDN (1B)
  For ISDN connections via one B channel, resolution 352 × 288/240 pixels
- Profile 7: Modem
  For analog modem connections at 20 kBit/s, resolution 352 × 288/240 pixels
- Profile 8: RAM recording
  Profile is linked to all RAM recordings, resolution 352 × 288/240 pixels

Active profile

Here you can select the desired profile for each of the two streams. You will see a preview for each data stream in the right section of the window. The preview of the data stream currently selected is marked by a frame. Various additional items of information regarding data transmission are displayed and continually updated above the previews.

– Click on a tab to select the associated stream.
– Select the desired setting from the list.

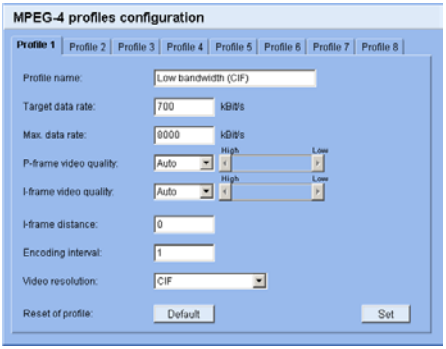
Note
Stream 2 is always transmitted for alarm connections and automatic connections. Take this into account when assigning the profile.

Preview for

Select which video data stream should be displayed in the previews. You can deactivate the display of the video images if the performance of the computer is affected too strongly by the decoding of the data streams.

Check the box for the required data stream.

Changing profiles



You can change individual parameter values within a profile and the name. You can switch between profiles by clicking the associated tabs.

Note
The profiles are rather complex. They include a number of parameters that interact with one another. Therefore it is generally best to use the default

profiles. The profiles should only be changed if you are completely familiar with all the configuration options.

Note
The parameters as a group constitute a profile and are dependent on one another. If you enter a setting outside the allowed range for a parameter, the nearest valid value is substituted when the settings are saved.

Profile name

You can enter a new name for the profile here. The name is then displayed in the list of available profiles in the Active encoder profile: field.

Target data rate

To optimize utilization of the bandwidth in your network, you can limit the data rate for the camera. The target data rate should be set according to the desired picture quality for typical scenes with no excessive motion.

For complex images or frequent changes of image content due to frequent movements, this limit can temporarily be exceeded as far as the value you enter in the Max. data rate: field.

Max. data rate

This maximum data rate is not exceeded under any circumstances. Depending on the video quality settings for the I- and P-frames this can result in the skipping of individual images.

The value entered here should be at least 10% higher than the value entered in the Target data rate field.

P-frame video quality

This setting allows you to adjust the image quality of the P-frames depending on the movement within the image. The Auto option automatically adjusts to the optimum relationship between movement and image definition (focus). Selecting Manual allows you to set a value between 4 and 31 on a slide bar. The value 4 represents the best quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of 31 results in a very high refresh rate and lower image quality.

I-frame video quality

This setting allows you to adjust the image quality of the I-frames. The Auto option automatically adjusts the quality to the settings for the P-frame video quality. Selecting Manual allows you to set a value between 4 and 31 on a slide bar. The value 4 represents the best quality with, if necessary, a lower frame refresh rate depending on the settings for the maximum data rate. A value of 31 results in a very high refresh rate and lower image quality.

I-frame distance

This parameter determines the number of inter-coded frames between two I-frames.

Encoding interval

The figure selected here determines the interval at which images are encoded and transmitted. For example, entering 4 means that only every fourth image is encoded, the following three images are skipped – this can be particularly advantageous with low bandwidths.

Video resolution

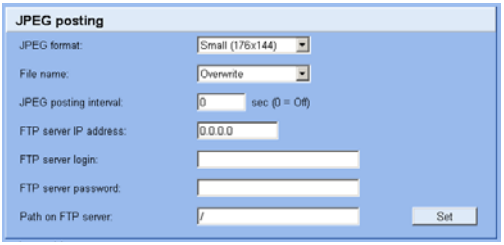
Here, you can select the desired resolution for the MPEG-4 video image. The following resolutions are available:

- QCIF 176 × 144/120 pixels
- CIF 352 × 288/240 pixels
- 1/2 D1 352 × 576/480 pixels
- 2CIF 704 × 288/240 pixels
- 4CIF/D1 704 × 576/480 pixels
- 2/3 D1 464 × 576/480 pixels

Profile reset

Click Default to return the profile to the factory default values.

JPEG posting



You can save individual JPEG images on an FTP server at certain intervals. You can then retrieve these images at a later date to reconstruct alarm events if required.

JPEG format

Select the resolution you wish the JPEG images to have:

- Small 176 × 144 pixels (QCIF)
- Medium 352 × 288 pixels (CIF)
- Large 704 × 576 pixels (4CIF)

File name

You can select how file names will be created for the individual images which are transmitted.

- Overwrite: The same file name is always used and any existing file will be overwritten with the current file.
- **Inc**rement: A number from 000 to 255 is added to the file name and automatically incremented by 1. When it reaches 255 it starts again from 000.
- Date/time suffix: The date and time are automatically added to the file name. When setting this parameter, please ensure that the date and time of the unit are always correctly set. Example: the file snap021606_124530.jpg was stored on February 16, 2006 at 12.45 p.m. and 30 seconds.

JPEG posting interval

Enter the interval in seconds at which the images will be sent to an FTP server. Enter zero if you do not want any images to be sent.

FTP server IP address

Enter the IP address of the FTP server on which you wish to save the JPEG images.

FTP server login

Enter your login name for the FTP server.

FTP server password

Enter the password that gives you access to the FTP server.

Path on FTP server

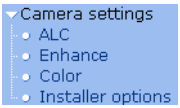
Enter the exact path on which you wish to post the images on the FTP server.

Post JPEG from camera

Check the box to activate one or more camera inputs for the JPEG image. An enabled camera input is indicated by a check mark.

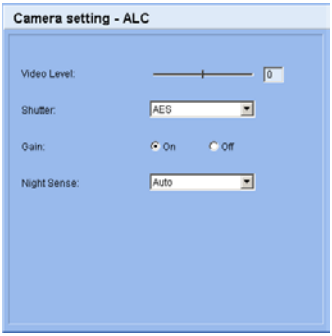
Note
The numbering follows the labeling of the video inputs on the actual unit.

Camera settings



Note
If the camera is in monochrome mode, all color related menu items are disabled and cannot be accessed.

ALC



Video level

Adjust the video output level (-15 to 0 to +15).

Shutter

- AES (auto-shutter) - the camera automatically sets the optimum shutter speed for manual iris lenses. The camera tries to maintain the selected shutter speed (1/60 [1/50], 1/100, 1/120, 1/250, 1/500, 1/1000, 1/2000, 1/5000, 1/10K) as long as the light level of the scene permits.
- FL - flickerless mode avoids interference from light sources (recommended for use with video iris or DC iris lenses only).

Gain

When the Gain mode is On, the camera automatically sets the gain to the lowest possible value needed to maintain a good picture.

NightSense™

Nightsense™ extends the low-light performance of the camera.

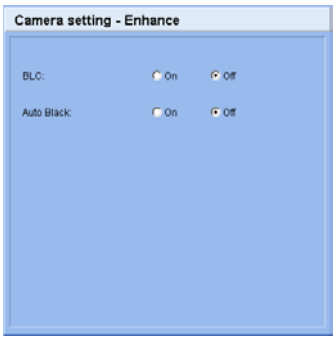
- In AUTO mode, the camera automatically inches to monochrome in low-light conditions.
- In FORCED mode, the camera remains in high-sensitivity monochrome operation.

Note

If NightSense™ is active, some noise or spots may appear in the picture. This is normal camera behavior. NightSense™ may cause some motion

blur on moving objects. If the camera is in monochrome mode, all color related menu items are disabled.

Enhance



Back Light Compensation (BLC)

When ON, the video level is optimized for the center of the image. Parts outside this area may be underexposed or overexposed (this is normal).

Auto Black

Autoblack ON automatically increases the visibility of details.

Color

White Balance

- ATW: Auto tracking white balance allows the camera to constantly adjust for optimal color reproduction.
- AWB HOLD: Puts the ATW on hold and saves the color settings.

Red Gain

Offset factory white point alignment (reducing red introduces more cyan).

Blue Gain

Offset factory white point alignment (reducing blue introduces more yellow).

Note

It is only necessary to change the white point offset for special scene conditions.

Installer options

Select the synchronization method for the camera: Internal for free running camera operation; Line Lock to lock to the power supply frequency.

You can disable the buttons on the camera to prevent unauthorized change of the camera settings. You can also disable the LED at the rear of the camera to avoid it interfering with the image sensing of the camera.

Click the Restore all defaults button to restore the factory defaults. A confirmation screen appears. Allow 5 seconds for the camera to optimize the picture after a mode reset.

Recording

You can record the images from the camera in the RAM memory of the unit or in an appropriately configured iSCSI storage device.

Local RAM memory is suitable for short-term recordings and pre-alarm recordings in Ring mode operation.

For long-term, authoritative images, it is essential that you use appropriately sized iSCSI storage.

Type

Select the desired storage medium to subsequently configure the recording parameters.

If you select RAM storage as the storage medium, the recording is started using Profile 8 immediately after you click the Set button. You can modify the settings of the this profile on the MPEG4 encoder page (see “Encoder Settings” on page 39). First, however, you must set Type to Off to stop all running recordings.

The preconfigured setting for Profile 8 is continuous ring recording with 8 MB storage size per channel and approximately 1 image per second in CIF format.

Caution

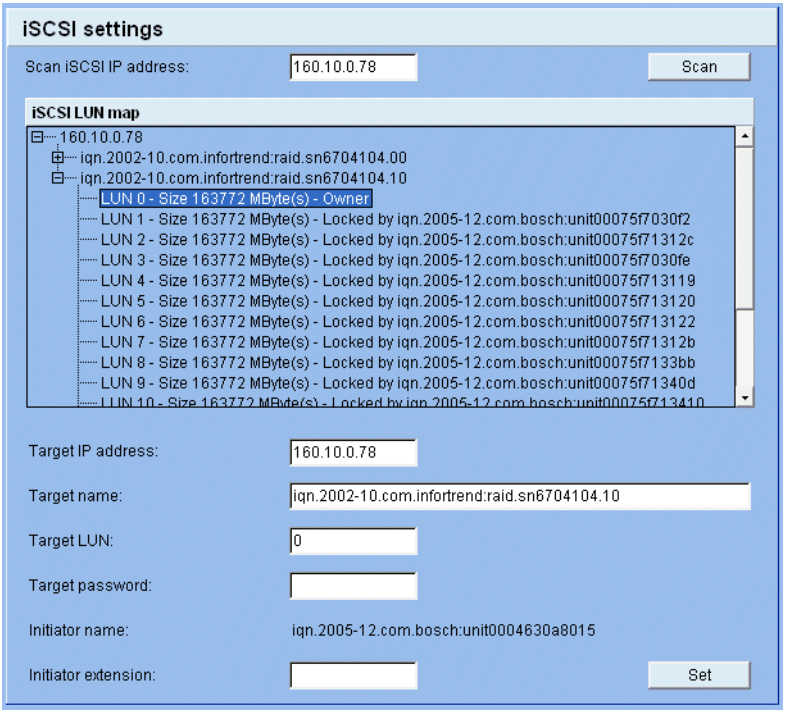
If you switch the storage medium from iSCSI server to RAM recording, the settings on the page iSCSI settings will be lost and can only be restored by reconfiguring them.

Storage information

The status of the currently selected storage medium and the data throughput are displayed here for information. You cannot change any of these settings.

- Click Advanced to view a status report with logged actions. A new window will open.
- In this window, click Delete to delete all entries. The entries will be deleted immediately; you cannot undo this process.
- Click the Close button to close the window.

iSCSI settings


iSCSI settings
Scan iSCSI IP address:
160.10.0.78
Scan
iSCSI LUN map
160.10.0.78
iqn.2002-10.com.infortrend:raid.sn6704104.00
iqn.2002-10.com.infortrend:raid.sn6704104.10
LUN 0 - Size 163772 MByte(s) - Owner
LUN 1 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f7030f2
LUN 2 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f71312c
LUN 3 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f7030fe
LUN 4 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f713119
LUN 5 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f713120
LUN 6 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f713122
LUN 7 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f71312b
LUN 8 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f7133bb
LUN 9 - Size 163772 MByte(s) - Locked by iqn.2005-12.com.bosch:unit00075f71340d
Target IP address:
160.10.0.78
Target name:
iqn.2002-10.com.infortrend:raid.sn6704104.10
Target LUN:
0
Target password:
Initiator name:
iqn.2005-12.com.bosch:unit0004630a8015
Initiator extension:
Set

If you select type iSCSI server as the storage medium, you then need to set up a connection to the desired iSCSI storage device and set the configuration parameters.

Note
The storage device selected must adhere to the iSCSI specification, be available on the network and be completely set up. Amongst other things, it must have an IP address and be divided into logical drives (LUN).

Scan iSCSI IP address

- Enter the IP address of the required iSCSI server here.
- Click the Scan button. The connection to the IP address will be established. The iSCSI LUN map field contains the corresponding logical drives.

iSCSI LUN map

The LUN map displays the logical drives configured for the iSCSI storage device. The current user is displayed for each drive.

- Double-click a free drive (LUN). The associated information is called up and automatically displayed in the fields below the map.
- If the logical drive is password protected, you must first enter the password in the Target password field and click the Set button.

Note
In cases where the information cannot be read due to the network topology, you must enter the data manually, so that the NWC-0495 can access the drive. In this case you should ensure that the entries correspond exactly with the configuration of the iSCSI device.

- After entering all the settings in the relevant fields, click Set. The NWC-0495 attempts to create a connection to the required drive using this data.

As soon as a connection has been established, the selected drive is used for recordings.

Target IP address

Enter the IP address of the required iSCSI server here.

Target name

Enter the name of the required drive.

Target LUN

Enter the LUN of the required drive.

Target password

If the drive is password protected, enter the password.

Note
You may not enter a new password. This is only possible by configuring the iSCSI storage device.

Initiator name

The initiator name is automatically displayed after a connection has been established.

Initiator extension

Enter the initiator extension. For the sake of clarity, you can enter a name or the existing extension with a comment, for example "– Camera 2"

Decoupling the drive used

Each drive can only be associated with one user. If a drive is already being used by another person, you can decouple the drive and connect the drive with the NWC-0495.

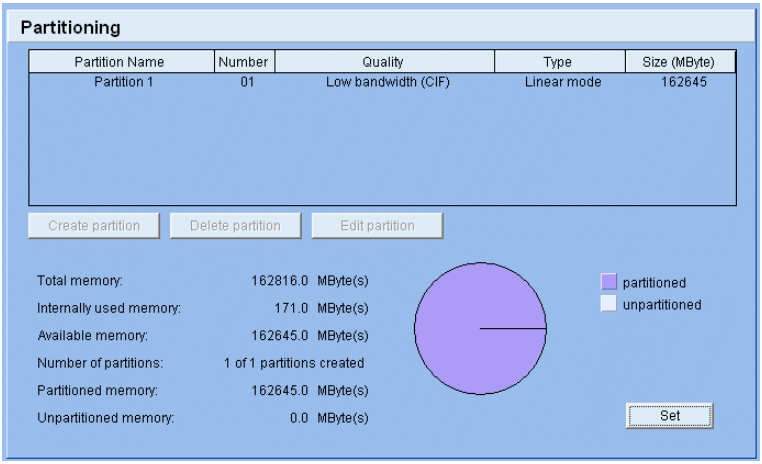
- Double-click a drive that is already being used in the LUN map. You will see a warning message.
- Confirm the decoupling of the current user. The drive is released and can be connected to the NWC-0495.

Storage information

The status of the currently selected storage medium and the data throughput are displayed here for information. You cannot change any of these settings.

- Click Advanced to view a status report with logged actions. A new window will open.
- In this window, click Delete to delete all entries. The entries will be deleted immediately; you cannot undo this process.
- Click the Close button to close the window.

Partitioning



A partition can be set up for recordings of the camera in a similar manner to the partitioning often found on computer hard drives. Parameters such as size, quality and type of video recording or compression standard used can be specified for the partition. Modifying these parameters leads to reorganization, during which stored data is lost.

In addition, the page provides you with an overview of the drive data; for example total memory. A pie chart indicates how much memory space is partitioned for recordings.

Creating a partition

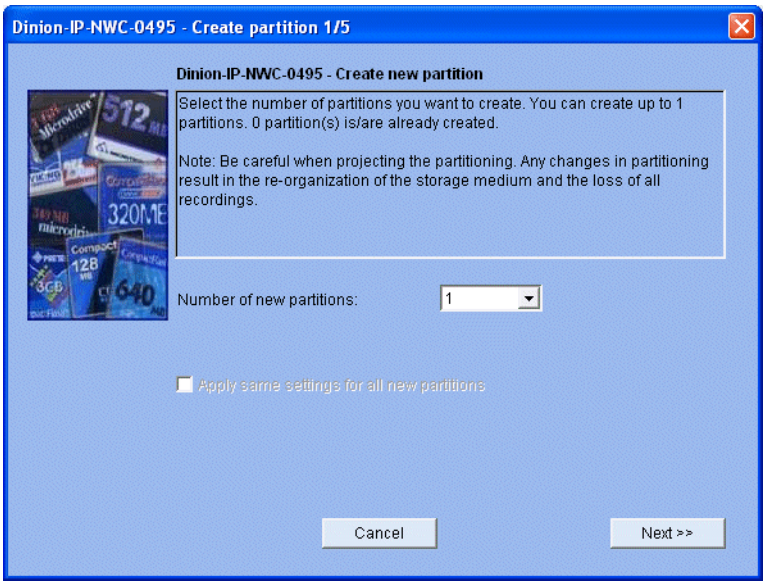
Caution

Modifications to the size of partitions lead to the entire hard drive being reorganized and the loss of all sequences stored on the drive.

Consequently, you should check the recordings before any modification to the parameters mentioned and back up important sequences on the computer's hard drive.

Creating a new partition is performed using separate windows in which information is presented to you and you are led step by step through the necessary settings.

- Click the Create partition button to start the assistant for creating partitions. The first window appears


Dinion-IP-NWC-0495 - Create partition 1/5
Dinion-IP-NWC-0495 - Create new partition
Select the number of partitions you want to create. You can create up to 1 partitions. 0 partition(s) is/are already created.
Note: Be careful when projecting the partitioning. Any changes in partitioning result in the re-organization of the storage medium and the loss of all recordings.
Number of new partitions:
1
Apply same settings for all new partitions
Cancel
Next >>

- You should always first read the information text in the upper section of the window.
- Click in the text fields to enter values or use the other controls that are available, such as buttons, checkboxes or list fields.
- Click the Next>> button in the lower section of the window to continue with the next step.
- Click the <<Back button in the lower section of the window to view the previous step again.
- Click the Cancel button to cancel the process and close the help.

Saving changes

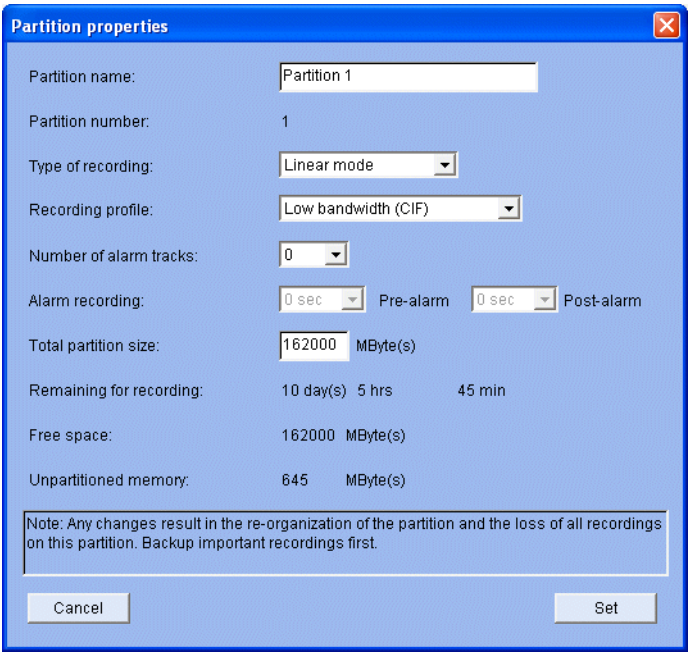
After you have made all necessary settings, you must transfer the settings to the unit and save them. To do this, you need to quit the help in the last window using the Finish button.

Caution

All modifications to settings are only effective if you complete the configuration in the last window by clicking Finish.

- Switch to the last window if necessary.
- Click Finish to complete the configuration. All settings are now transferred to the unit and subsequently become effective.

Editing a partition



You can modify the configuration of a partition at any time.

Caution

All modifications result in the re-organization of the partition and the loss of all sequences on this partition. Changes to the size of a partition (Total partition size) lead to the entire hard drive being reorganized and the loss of all recordings stored on the drive. Consequently, you should back up all important sequences on the computer's hard drive before modifying the partition.

You can perform the required modifications in the Partition properties window.

- Click the Edit partition button. A new window with the entries for the selected partition is opened.
- Enter the necessary changes.
- Click the Set button to save the modifications.
- After closing the window, click the Set button in the main window to transfer the changes to the unit and to save them.

Deleting partitions

You can delete a partition at any time.

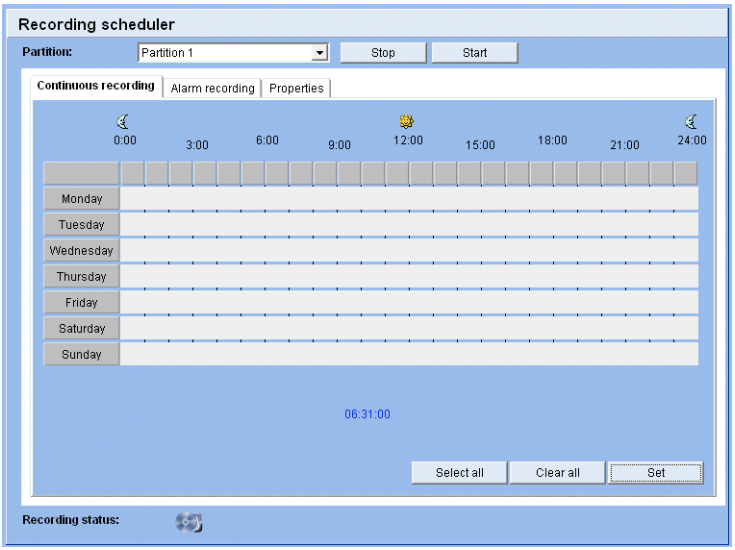
Caution

Deleting a partition leads to the entire hard drive being reorganized and loss of all sequences stored on the drive. Consequently, you should check the recordings before deleting any partition and back up important sequences on the computer's hard drive.

- Click the Delete partition button to delete the highlighted partition. The line containing the associated number remains in the display, the partition name is deleted and the size is indicated as 0.
- Click the Set button to transfer the changes to the unit and to save them.

Recording scheduler

Set all parameters for recording. Recording can be performed continuously or in the case of an alarm.



Activating a partition for recording

After configuration, you can activate the partition for recording by clicking the Start button.

After starting, the pages Continuous recording, Alarm recording and the Properties for the activated partitions are displayed in gray, and the configuration cannot be modified.

The graphic in the lower section of the pages indicates this partition's recording activity. You will see an animated graphic while recording is taking place. You can terminate recording at any time and deactivate the partition.

- Click the Start button to activate the currently selected partition for recording.
- Click the Stop button to deactivate the currently selected partition for recording. Recordings that are currently running will be interrupted and the configuration can be modified.

Continuous recording

You can specify the times during which continuous recording to the hard drive should take place.

Separate selection fields are available for each day of the week. You can select up to 16 individual recording time intervals for each day of the week.

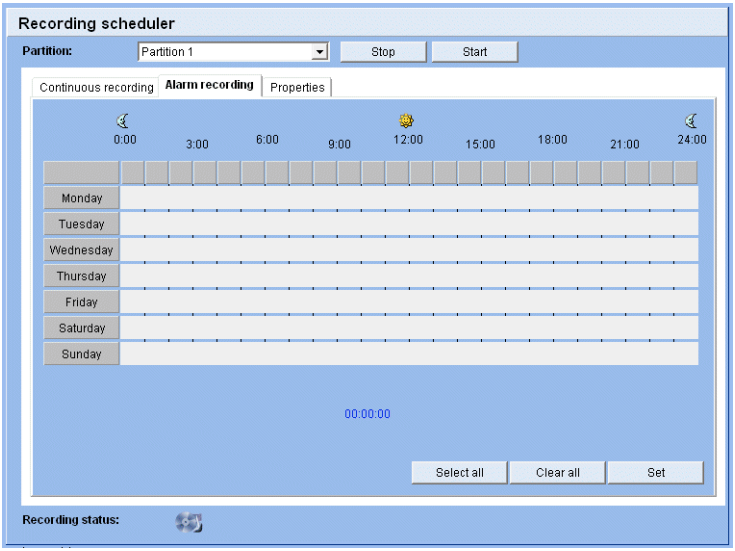
Note
If a time interval has already been selected for alarm recording, you cannot select it for continuous recording (see "Alarm recording" on page 59).

- Left-click the point in the schedule at which recording should start and hold the button down.
- Drag the selected field to the desired recording end and then release the mouse key.
- Right-click a highlighted time interval to delete it.
- Click the Select all button to highlight all time intervals.
- Click the Clear all button to delete all highlighted time intervals.

Recording status

The graphic indicates the recording activity in this partition. You will see an animated graphic while recording is taking place.

Alarm recording



You can specify the times during which images from the camera should be recorded in the event of an alarm.

You can select up to 16 individual recording time intervals for each day of the week. Alarm recording occurs only during the highlighted time intervals.

Note

If a time interval has already been selected for continuous recording, you cannot select it for alarm recording (see "Continuous recording" on page 58).

Caution

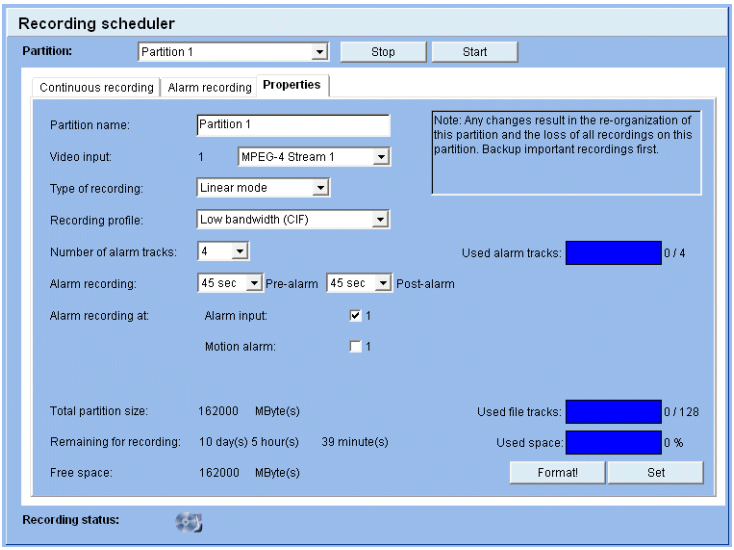
Alarm tracks must be set up in the required partition for alarm recording (see "Number of alarm tracks" on page 61).

The unit uses a special recording mode during alarm recording for optimal usage of storage capacity: as soon as a time gap for alarm recording begins, a recording is continuously made on one segment, which is the size of a complete alarm sequence (pre- and post-alarm time).

This segment in the partition functions in a similar manner to a ring buffer and is overwritten until an alarm is actually triggered. Recording occurs on the segment only for the duration of the preset post-alarm time and a new segment subsequently used in the same manner.

This ensures that the alarm recorded is always secured for its entire duration and the space required to save each alarm recording is easy to calculate.

Properties



You can view the current properties directly in the recording scheduler and modify them if necessary. You can also activate the alarms that should trigger recording. Similarly, you can also select the profile for recording.

Caution

All modifications result in the re-organization of the partition and the loss of all sequences on this partition. Changes to the size of a partition (Total partition size) lead to the entire hard drive being reorganized and the loss of all recordings stored on the drive. Consequently, you should back up all important sequences on the computer's hard drive.

Partition name

You can enter a new name for the partition.

Video input

The number of the video input is displayed for information purposes.

- Select the required data stream from the list field.

Type of recording

Select the required recording type.

In the case of ring mode the recording proceeds continuously. If the maximum hard drive space has been reached, the oldest recordings are automatically overwritten.

In the case of linear mode the recording proceeds until the entire hard drive space is full. The recording is then stopped until old recordings have been deleted.

Recording profile

Select the profile that is to be active during recording. You can view and modify the parameters for the profile (see “Encoder Settings” on page 39).

Note
The recording profile can deviate from the standard setting Active profile for the video input set and is only used during an active recording.

Number of alarm tracks

Select the number of alarm tracks to be used in the partition. One alarm event can be recorded in each alarm track. Accordingly, the number of alarms entered can be recorded and archived. A partition can contain a maximum of 128 alarm recordings.

If the option ring mode is set for a partition, the latest alarm recordings are always saved in the preset number. If the option linear mode is selected, the recording is stopped as soon as the total number of alarm tracks has been recorded.

Already Used alarm tracks are displayed in the graphic next to the parameter.

Alarm recording

Select which time intervals are to be covered for Pre-alarm and Post-alarm.

Alarm recording at

You can select the alarm sensor to trigger a recording. You can also use the motion alarm to trigger the alarm recording.

Note

The alarm sensor must be active to be able to trigger the recording. The alarm input is activated on the page Alarm sources (see "Alarm in" on page 63). The motion alarm is configured and activated on the page Video content analysis (see "Video content analysis" on page 65).

- Check the box for the alarm sensor that is to trigger a recording. The alarm sensors selected are indicated by a check mark.

This displays how much storage space the partition occupies on the drive.

Already Used file tracks are displayed in the graphic next to the parameter.

Remaining for recording

This displays the maximum remaining recording time. The value is automatically updated after the parameters have been modified.

Free space

This displays how much space is still available in the partition.

Used space

This displays how much space is already used in the partition.

Format!

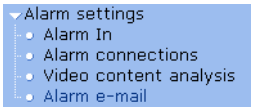
You can delete all recordings in a partition at any time.

Caution

Check the recordings before deleting and back up important sequences on the computer's hard drive.

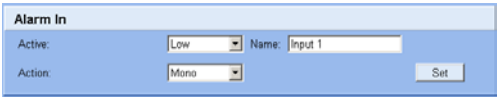
- Click the Format! button to delete all recordings in the currently selected partition.

Alarm Settings



Here, you can make the settings for the alarm sources and alarm connections.

Alarm in



You can configure the possible alarm triggers for the camera.

Alarm input Select Active Low if the alarm is to be triggered by closing the contact. Select Active High if the alarm is to be triggered by opening the contact.

Action

Select how the camera responds to an incoming alarm. The camera can either switch the camera settings profile (not the recordings profile) or switch to Night mode. If None is selected, the alarm will only be forwarded via the IP connection.

Name

You can enter a name for each alarm input, which is then displayed below the icon for the alarm input on the Livepage during configuration.

Alarm connections

You can select the response of the camera in case of an alarm. In case of an alarm, the camera can automatically establish a connection to a predefined IP address (compatible MPEG-4 compatible hardware receiver or computer with reception

software). You can enter up to ten IP addresses which will be selected in order by the unit in case of an alarm until a connection is established.

Connect on alarm

Select On so that the camera automatically establishes a connection to a pre-defined IP address in the event of an alarm.

Note
Stream 2 is always transmitted for alarm connections. This should be taken into account when assigning the profile.

Number of destination IP address

Here you assign the numbering for the IP addresses to be contacted in the event of an alarm. The unit contacts the remote locations one after the other in the numbered sequence until a connection has been established.

Destination IP address

For each number, enter the corresponding IP address for the desired remote location.

Destination password

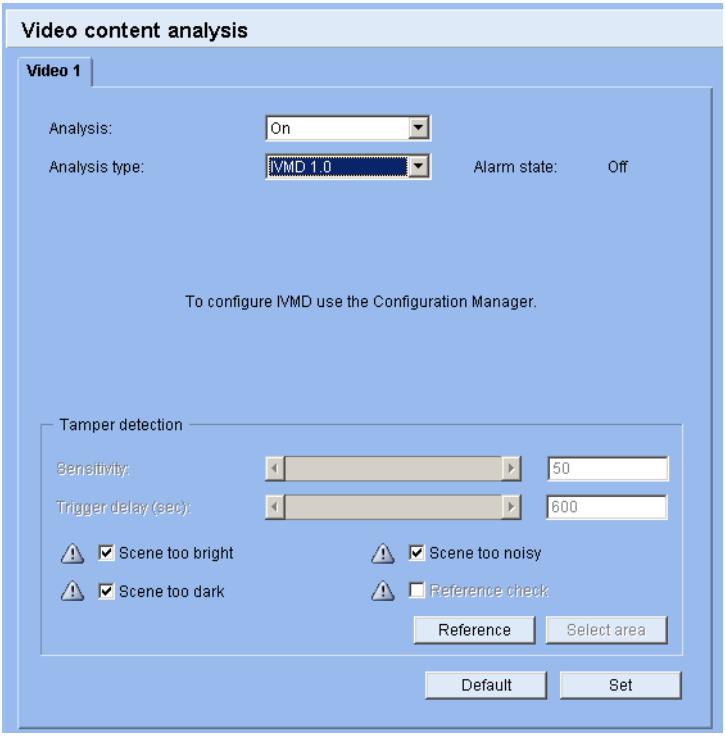
If the remote location is password protected, enter the password here.

Auto-connect

Select On if an active connection should be re-established automatically to one of the previously specified IP addresses after each restart, connection breakdown or network failure.

Note
Stream 2 is always transmitted for automatic connections. This should be taken into account when assigning the profile.

Video content analysis



The NWC-0495 contains an integrated Video Content Analysis (VCA), which can detect and analyze changes in the signal. Such changes can be due to movements in the camera's field of view.

You can configure the video content analysis for the camera.

If necessary, click the Default button to return all settings to their default values.

Analysis

Select the option On to activate the video content analysis.

As soon as the video content analysis is activated, metadata are created. Depending on the Analysis type selected and the relevant configuration, additional information overlays the video image in the small window. If you have selected MOTION+ analysis, for example, the sensor fields will light up in which movement is registered.

Note
On the Livepage configuration page, you can enable additional information overlays for the live video image too (see "Livepage configuration" on page 76).

Analysis type

Select the required analysis algorithm. By default, only MOTION+ is available – this offers a motion detector and essential recognition of tampering. The current alarm status is displayed for information purposes.

Note
Additional analysis algorithms with comprehensive functions such as IVMD are available from Bosch Security Systems.

Motion detector

For the detector to function, the following conditions must be met:

- Analysis must be activated.
- At least one sensor field must be activated.
- The individual parameters must be configured to suit the operating environment and the desired responses.
- The sensitivity must be set to a value greater than zero.

Caution
Reflections of light (off glass surfaces, etc.), switching lights on or off or changes in the light level caused by cloud movement on a sunny day can trigger unintended responses from the motion detector and generate false alarms. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.
For indoor surveillance, ensure constant lighting of the areas during the day and at night.

Sensitivity

The basic sensitivity of the motion detector can be adjusted for the environmental conditions to which the camera is subject.

The sensor reacts to variations in the brightness of the video image. The darker the observation area, the higher the value that must be selected.

Min. object size

You can specify the number of sensor fields that a moving object must cover to generate an alarm. This setting prevents objects that are too small from triggering an alarm.

A minimum value of 4 is recommended. This value corresponds to four sensor fields.

Selecting the area

The areas of the image to be monitored by the motion detector can be selected. The video image is subdivided into 858 square sensor fields. You can activate or deactivate each of these fields individually. If you wish to exclude particular regions of the camera's field of view from monitoring due to continuous movement (by a tree in the wind, etc.), the relevant fields can be deactivated.

- Click Select area to configure the sensor fields. A new window will open.
- If necessary, click Clear all first to clear the current selection (fields marked red).
- Left-click the fields to be activated. Activated fields are marked red.
- If necessary, click Select all to select the entire video frame for monitoring.
- Right-click any fields you wish to deactivate.
- Click OK to save the configuration.
- Click the close button (X) in the window title bar to close the window without saving the changes.

Tamper detection

You can reveal the tampering of cameras and video cables by means of various options. Run a series of tests at different times of the day and night to ensure that the video sensor is operating as intended.

Note

The options for tamper detection can only be set for fixed cameras. Dome cameras or other motorized cameras cannot be protected in this manner as

the movement of the camera itself causes changes in the video image that are too big.

Global change %

You can define the percentage of sensor fields that must register a change simultaneously before generating an alarm. This setting is independent of the sensor fields selected under Select area.

This option allows you to detect, independently of motion alarms, manipulation of the orientation or location of a camera resulting from turning the camera mounting bracket, for instance.

Sensitivity

Note
This and the following parameter are only accessible if the reference check is activated.

The basic sensitivity of the tamper detection can be adjusted for the environmental conditions to which the camera is subject.

The algorithm reacts to the differences between the reference image and the current video image. The darker the observation area, the higher the value that must be selected.

Trigger delay

You can set delayed alarm triggering. The alarm is only triggered after a set time interval in seconds has elapsed and then only if the triggering condition still exists. If the original condition has been restored before this time interval elapses, the alarm is not triggered. This allows you to avoid false alarms triggered by short-term changes, for example cleaning activities in the direct field of vision of the camera.

Scene too bright

Activate this function if tampering associated with exposure to extreme light (for instance, shining a flashlight directly on the objective) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

Scene too dark

Activate this function if tampering associated with covering the objective (for instance, by spraying paint on it) should trigger an alarm. The average brightness of the scene provides a basis for recognition.

Scene too noisy

Activate this function if tampering associated with EMC interference (noisy scene as the result of a strong interference signal in the vicinity of the video lines), as an example, should trigger an alarm.

Reference check

You can save a reference image that is continuously compared with the current video image. If the current video image in the marked areas differs from the reference image, an alarm is triggered. This allows you to detect tampering that would otherwise not be detected, for example if the camera is turned.

- Click Reference to save the currently visible video image as a reference.
- Click Select area and select the areas in the reference image that are to be monitored.
- Check the box Reference check to activate the on-going check. The stored reference image is displayed in black and white below the current video image, and the selected areas are marked in red.

Selecting the area

You can select the image areas in the reference image that are to be monitored. The video image is subdivided into 858 square fields. You can activate or deactivate each of these fields individually.

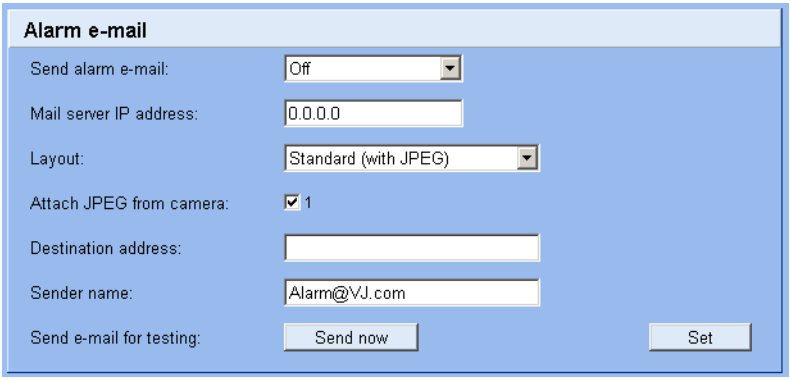
Note

Select only those areas for reference monitoring in which no movement takes place and that are always evenly lit, as false alarms could otherwise be triggered.

- Click Select area to configure the sensor fields. A new window will open.
- If necessary, click Clear all first to clear the current selection (fields marked red).
- Left-click the fields to be activated. Activated fields are marked red.

- If necessary, click Select all to select the entire video frame for monitoring.
- Right-click any fields you wish to deactivate.
- Click OK to save the configuration.
- Click the close button (X) in the window title bar to close the window without saving the changes.

Alarm e-mail



As an alternative to automatic connecting, alarm states can also be documented by e-mail. In this way it is possible to notify a recipient who does not have a video receiver. In this case the NWC-0495 automatically sends an e-mail to a user defined e-mail address.

Send alarm e-mail

Select On if you want the unit to automatically send an alarm e-mail in the event of an alarm.

Mail server IP address

Enter the IP address of a mail server that operates on the SMTP standard (Simple Mail Transfer Protocol). Outgoing e-mails are sent to the mail server via the address you entered. Otherwise leave the box blank (0.0.0.0).

Layout

You can select the data format of the alarm message.

- Standard (with JPEG): e-mail with JPEG image file attachment.
- SMS: e-mail in SMS format to an e-mail-to-SMS gateway (for example to send an alarm by cellphone) without an image attachment.

Caution

When a cellphone is used as the receiver, make sure to activate the e-mail or SMS function, depending on the format, so that these messages can be received. You can obtain information on operating your cellphone from your cellphone provider.

Attach JPEG from camera

Click the checkbox to select the cameras from which JPEG images are sent. An enabled video input is indicated by a check mark.

Destination address

Enter the e-mail address for alarm e-mails here. The maximum address length is 49 characters.

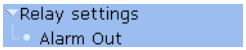
Sender name

Enter a unique name for the e-mail sender, for example the location of the unit. This will make it easier to identify the origin of the e-mail.

Send e-mail for testing

Test the e-mail function by clicking the Send now button. An alarm e-mail is immediately created and sent.

Relay Settings



Here, you can make the settings for the alarm sources and alarm connections.

Alarm out

Select the event that will trigger the alarm output;

- an internal motion detection/VCA,
- an internal day/night switching, or
- an external trigger from the network.

For example, it is possible to switch on a spotlight in response to a motion alarm and switch it off again when the alarm is over.

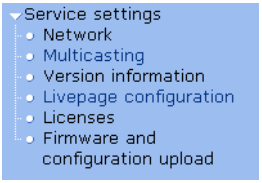
Relay name

The relay can be assigned a name here. The name is shown on the button next to Trigger relay. The Livepage can also be configured to display the name next to the relay icon.

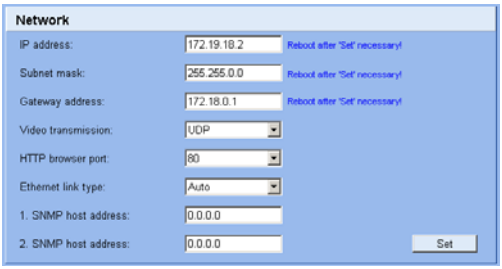
Trigger relay

Click the button to switch the relay manually (for example for testing purposes or to operate a door opener).

Service Settings



Network



The settings on this page are used to integrate the unit into an existing network.

Note
Changes to the IP address, subnet mask or gateway address are transferred to the unit by clicking Set.

– Click Set after entering a new IP address.
– To do this, enter the old IP address followed by `/reset` (for instance `192.168.0.80/reset`) in the address bar of your web browser. When the camera is restarted it can only be accessed at the new IP address.

IP address

Enter the desired IP address for the camera in this field. The IP address must be valid for the network.

Subnet mask

Enter the appropriate subnet mask for the set IP address here.

Gateway address

If you want the unit to establish a connection to a remote location in a different subnet, enter the IP address of the gateway here. Otherwise, this field can remain empty (0.0.0.0).

HTTP browser port

Select a different HTTP browser port from the list if required. The default HTTP port is 80.

Video transmission

If the unit is used behind a firewall, TCP (Port 80) should be selected as the transmission protocol. For use in a local network, choose UDP.

Note

Multicast operation is only possible with the UDP protocol. The TCP protocol does not support multicast connections. The MTU value in UDP mode is 1514 bytes.

Ethernet link type

If the camera is connected to the network via a switch, both devices must have the same preset network connection type. If necessary, ask your network administrator what value the associated switch is set to.

Choose Auto for an autosensing network connection. If necessary you can set the value to 10 or 100 MBit/s for either full or half-duplex mode (FD or HD).

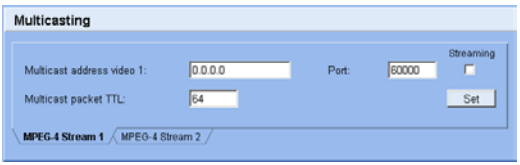
Note

Malfunctions can occur (for example image faults) if the network capacity is not sufficient for transmission of the maximum data rate generated by the camera.

1. SNMP host address / 2. SNMP host address

The NWC-0495 supports the SNMP (Simple Network Management Protocol) for managing and monitoring network components, and can send SNMP messages to IP addresses. It supports SNMP MIB II and its traps in their full functionality in the unified code. If you wish to send SNMP traps, enter the IP addresses of one or two required target devices here.

Multicasting



In addition to a 1:1 connection between an encoder and a single receiver (unicast), the camera can enable multiple receivers to receive the video signal from an encoder simultaneously. This is either done by duplicating the data

stream in the unit and then distributing it to multiple receivers (multi-unicast) or by distributing an individual data stream in the network itself to multiple receivers in a defined group (multicast). You can enter a dedicated multicast address and port for each stream. You can switch between the streams by clicking the associated tabs.

Note
The prerequisite for multicast operation is a multicast-capable network that uses the UDP and IGMP protocols. Other group membership protocols are not supported. The TCP protocol does not support multicast connections.

A special IP address (class D address) must be configured for multicast operation in a multicast-enabled network. The network must support group IP addresses and the Internet Group Management Protocol (IGMP V2). The address range is from 225.0.0.0 to 239.255.255.255. The multicast address can be the same for multiple streams. However, it is then necessary to use a different port in each case so that multiple data streams are not sent simultaneously using the same port and multicast address.

Multicast address video 1

Enter a valid multicast address for each stream to be operated in multicast mode (duplication of the data streams in the network). With the setting 0.0.0.0 the encoder for the relevant stream operates in multi-unicast mode (copying of data streams in unit). The camera supports multi-unicast connections for up to five simultaneously connected receivers.

Note
Duplication of data places a heavy demand on the CPU and can lead to impairment of the image quality under certain circumstances.

Port

If there are simultaneous data streams at the same multicast address, you must assign different ports to each data stream. Enter the port address for the relevant stream here.

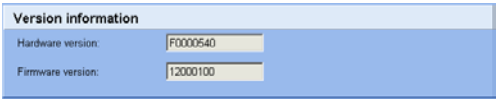
Streaming

Click in the check box to activate multicast streaming mode for the relevant stream. An activated stream is marked with a check.

Multicast packet TTL

A value can be entered to specify how long the multicast data packets are active on the network. If multicast is to be run via a router the value must be greater than 1.

Version information



The hardware and firmware version numbers are for information only and cannot be altered. Keep a record of these numbers in case technical assistance is required.

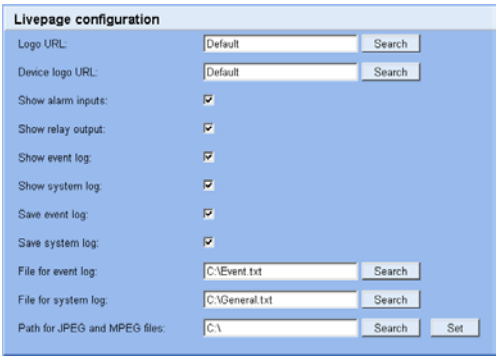
Hardware version

The hardware version number of the camera is displayed.

Firmware version

The firmware version number of the camera is displayed.

Livepage configuration



In this window, you can adapt the appearance of the Livepage to meet your requirements. Options are provided here to display various information and

operating elements in addition to the video image. Moreover, individual background graphics can be used for the main window and the upper area of the window (banners).

Note
Either GIF or JPEG images can be used. The file paths must correspond to the access mode (for example `C:\Images\Logo.gif` for access to local files or `http://www.myhostname.com/images/logo.gif` for access via the Internet/Intranet).

For access via the Internet/Intranet, there must be a connection in order to display the image. The image files are not stored on the camera.

– Mark the check boxes for the information to be displayed on the Livepage. The selected elements are checked.
– Check on the Livepage whether and how the desired items are displayed.

Logo URL

Enter the path to a suitable background graphic in this field. The image can be stored on a local computer, a local network or at an Internet address.

– Click Search if necessary to find a suitable image on the local network.

Device logo URL

Enter the path for a suitable image for the upper part of the window (banner) here. The image can be stored on a local computer, a local network or at an Internet address.

– Click Search if necessary to find a suitable image on the local network.

Note
To restore the original graphics, simply delete the entries in the Logo URL and Device logo URL fields.

Show alarm input

Alarm inputs are displayed next to the video image as icons along with their assigned names. If an alarm is active the corresponding icon changes color.

Show event log

The event messages are displayed with the date and time in a field next to the video image.

Show system log

The system messages are displayed with the date and time in a field next to the video image and provide information about the establishment and termination of connections etc.

Save event log

Select this option to save event messages in a text file on the local computer. This file can be viewed, edited and printed with any text editor or the standard Office software.

Save system log

Select this option to save system messages in a text file on the local computer. This file can be viewed, edited and printed with any text editor or the standard Office software.

File for event log

Enter the path for saving the event log here.

– If necessary, click Search to find a suitable folder.

File for system log

Enter the path for saving the system log here.

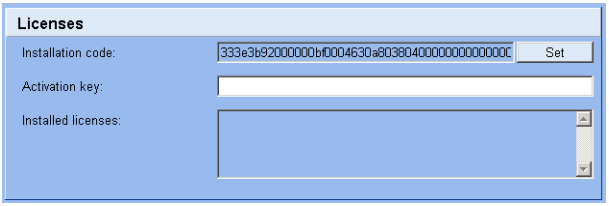
– If necessary, click Search to find a suitable folder.

Path for JPEG and MPEG files

Enter the path for the storage location of individual images and video sequences that you can save from the Livepage.

– If necessary, click Search to find a suitable folder.

Licenses

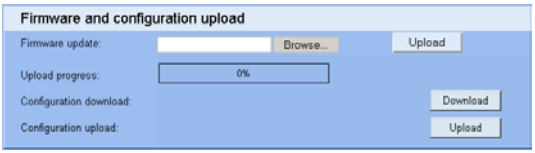


You can enter the activation key to release additional functions or software modules.

Note

The activation key cannot be deactivated again and is not transferable to other units.

Firmware and configuration upload



Firmware update

The camera functions and parameters can be updated with firmware. To do this, the current firmware package is transferred to the unit via the network. The firmware is installed there automatically. Thus a camera can be serviced and updated remotely without requiring a technician to make changes to the unit on site. The latest firmware can be obtained from your customer service center or from the Bosch Security Systems download area.

Caution

Before starting the firmware update, make sure that you have selected the correct upload file! Uploading the wrong files can result in the unit no longer being addressable, requiring it to be replaced.

Caution

Do not interrupt the firmware installation for any reason! Interruption may lead to faulty coding of the Flash EPROM. This can result in the unit no longer being addressable, requiring it to be replaced.

Note

A firmware update resets all camera parameters to their factory default values. If you wish to retain the old values first save the configuration by performing a configuration download. After the firmware update you can reload your parameter values by performing a configuration upload.

To update the firmware:

- First, save the update file to the hard disk.
- Enter the full path for the update file in the field or click Browse... to locate and select the file.
- Click Upload to begin transmission to the unit. The progress bar allows you to monitor the transfer.

Note

Installing new firmware and reconfiguring the camera takes several minutes.

The new firmware is unpacked and the Flash EPROM is reprogrammed. The time remaining is shown by the message going to reset Reconnecting in ... seconds. After the upload is completed successfully, the unit will restart automatically.

If the operating status LED lights up red, the upload has failed and must be repeated. To perform the upload, you must switch to a special page:

- In the address bar of your browser, after the unit IP address enter `/main.htm` (for example `192.168.0.80/main.htm`).
- Repeat the upload.

Configuration download

You can save configuration data for the camera to a computer and load saved configuration data from a computer to the unit.

– Click Download; a dialog box appears.
– Follow the instructions to save the current settings.

Configuration upload

– Enter the full path of the file to upload or click Browse... to select the desired file.
– Make certain that the file to be loaded comes from the same device type as the unit you want to reconfigure.
– Click Upload to begin transmission to the unit. The progress bar allows you to monitor the transfer.

Once the upload is complete, the new configuration is activated. The time remaining is shown by the message going to reset Reconnecting in ... seconds. After the upload is completed successfully, the unit will restart automatically.

Function test

The camera offers a variety of configuration options. Therefore you should check that it works properly after installation and configuration. This is the only way to ensure that the camera will function as intended in the event of an alarm.

Your check should include the following functions:

- Can the camera be called remotely?
- Does the camera transmit all the data required?
- Does the camera respond as desired to alarm events?
- Is it possible to control peripheral devices if necessary?

7 Connections between video servers

A camera can be used as a transmitter and a compatible MPEG-4 hardware decoder with a connected monitor as a receiver using an Ethernet network connection. This way it is possible to cover large distances with little effort for installation or cabling.

Installation

Cameras are designed to connect with other VIP devices automatically with the corresponding configuration. This only requires that they are part of a closed network. Proceed as follows to install the devices:

– Connect the devices to the closed network using Ethernet cables.

– Connect them to the power supply.

Note

Make sure the devices are configured for the network environment and the correct IP address for the remote location to be contacted in the event of an alarm is set on the Alarm connections configuration page.

Establishing the connection

There are three options for establishing a connection between a transmitter and a compatible receiver in a closed network:

- an alarm,
- a Web browser
- via the configuration manager

Connect on alarm

With the appropriate configuration, a connection between a transmitter and a receiver is established automatically when an alarm is triggered. After a short time, the live video image from the transmitter is shown on the connected monitor.

This connection option can also be used to connect a transmitter and a compatible receiver using a switch connected to the alarm input. In this case, no computer is needed to establish the connection.

Connecting with a Web browser

Various requirements must be met in order to operate using a Web program.

Note
Transmitter and receiver must be located in the same subnet to establish a hardware connection with a Web browser.

– Use the Web browser to connect to the receiver. Its home page is displayed.
– Under Video sources on the page Connections, select the camera. A JPEG snapshot of the video source selected is displayed on the page.
– Click MPEG-4 connection to begin displaying the video images on the connected monitor.

Closing the connection

The connection may be closed using a Web browser.

– Use the Web browser to connect to the receiver. Its home page is displayed.

In the title bar of the Monitor window on the page Connections, click on the X icon to end the display of the video images on the connected monitor.

8 Operation with decoder software

The camera video server and VIDOS software combine to provide a high-performance system solution.

VIDOS is software for operating, controlling and administering CCTV installations (such as surveillance systems) at remote locations. It runs under Microsoft Windows operating systems. Its main job is decoding video, audio and control data from a remote transmitter.

There are many options available for operation and configuration operation when using a camera with VIDOS. Refer to the software documentation for more details.

The camera is also designed to operate with the DIBOS 8.0 digital recorder platform.

9 Maintenance

Testing the network connection

The `ping` command can be used to check the connection between two IP addresses. This allows you to test whether a device is active in the network.

– Open the DOS command prompt.

– Type `ping` followed by the IP address of the device.

If the device is found, the response appears as "`Reply from ...`", followed by the number of bytes sent and the transmission time in milliseconds. Otherwise, the device cannot be accessed via the network. This might be because:

- The device is not properly connected to the network. Check the cable connections in this case.
- The device is not correctly integrated into the network. Check the IP address, subnet mask and gateway address.

Repairs

Caution

Never open the casing of the camera. The unit does not contain any user serviceable parts.

Ensure that all maintenance or repair work is performed only by qualified personnel (electrical engineering or network technology specialists). In case of doubt, contact your dealer's technical service center.

Transfer and disposal

The camera should only be passed on together with this installation guide. The unit contains environmentally hazardous materials that must be disposed of according to law. Defective or superfluous devices and parts should be disposed of professionally or taken to your local collection point for hazardous materials.

10 Troubleshooting

If you cannot resolve a fault, please contact your supplier or system integrator or go direct to Bosch Security Systems Customer Service.

The version numbers of the internal processors can be viewed on a special page. Please note this information before contacting Customer Service.

– In the address bar of your browser, after the unit IP address enter `/version` (for example `192.168.0.80/version`).
– Write down the information or print out the page.

The following table is intended to help you identify the causes of malfunctions and correct them where possible.

Malfunction	Possible causes	Solution
No image transmission to remote location.	Defective camera.	Connect a local monitor to the camera and check the camera function.
	Faulty cable connections.	Check all cables, plugs, contacts and connections.
No connection established, no image transmission.	The unit's configuration.	Check all configuration parameters.
	Faulty installation.	Check all cables, plugs, contacts and connections.
	Wrong IP address.	Check the IP addresses (terminal program).
	Faulty data transmission within the LAN.	Check the data transmission with `ping`.
	The maximum number of connections has been reached.	Wait until there is a free connection and call the transmitter again.
The unit does not report an alarm.	Alarm source is not selected.	Select possible alarm sources on the Alarm sources configuration page.
	No alarm response specified.	Specify the desired alarm response on the Alarm connections configuration page, if necessary change the IP address.

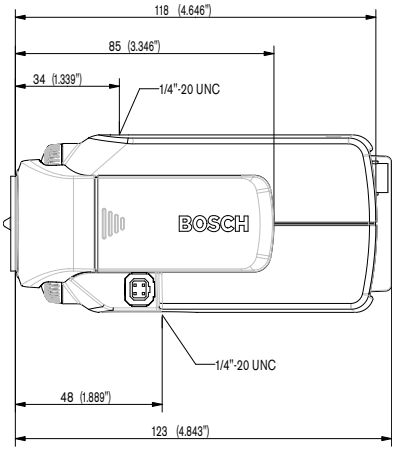
Malfunction	Possible causes	Solution
The unit is not operational after firmware upload.	Power failure during programming by the update file.	Have the unit checked by Customer Service and replace if necessary.
	Incorrect update file.	Enter the IP address followed by `/main.htm` in your web browser and repeat the upload.

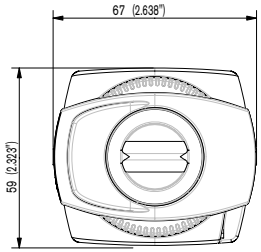
11 Specifications

Type number	NWC-0495-10P	NWC-0495-20P
Standard	PAL	NTSC
Active pixels	752x582	768x492
Rated supply voltage	24 VAC or 12 VDC or Power-over-Ethernet (IEEE 802.3af) 12-28 VAC (50/60 Hz) 11-36 VDC	
Min illumination	< 0.4 lux < 0.15 lux (in monochrome mode)	
Imager	Interline CCD	
Resolution	540 TVL (BNC)	
SNR	> 50 dB	
Video output	1 Vpp, 75 Ohm	
Synchronization	Internal or Line Lock selectable	
Shutter	AES (1/60 (1/50) to 1/100000), Flickerless, Fixed selectable	
Sens Up	Adjustable from OFF to 10x	
Auto black	On, Off selectable (maximum level selectable up to 28dB)	
BLC	BLC On or Off selectable	
White balance	Automatic 2500 - 9000K (with AWB hold mode and manual mode)	
Color saturation	Adjustable from monochrome (0%) to 133% color	
Lens Mount	CS compatible, C-mount compatible with supplied adapter ring	
ALC lens	Video or DC iris auto detect	
Power consumption	< 8 W	
Dimensions	59 x 67 x 122 mm (2.28 x 2.6 x 4.8 inch) without lens (HxWxL)	
Weight	450g (0.99 lbs) without lens	
Tripod Mount	Bottom (isolated) and Top ¼" 20 UNC	
Operating temperature	0° to 40° C (32° to 104° F)	
Controls	OSD with softkey operation	
LAN interface	1 × Ethernet 10/100 Base-T, automatic adaptation, half/full duplex, RJ-45	
Video encoding protocols	MPEG-4, JPEG	
Video data rate	9,600 KBit/s ... 10 MBit/s	

Image resolutions (PAL/NTSC)	704 × 576/480 pixels (D1/4CIF) 464 × 576/480 pixels (2/3 D1) 704 × 288/240 pixels (2CIF) 704 × 288/240 pixels (1/2 D1) 352 × 288/240 pixels (CIF) 176 × 144/120 pixels (QCIF)
Total delay	120 ms (PAL/NTSC, MPEG-4, no network delay)
Image refresh rate Field/image-based coding	1 ... 50/60 fields/s adjustable (PAL/NTSC)
Network protocols	TCP, UDP, IP, HTTP, IGMP V2, ICMP, ARP

Dimensions





Dimensions in mm (inches).

12 Accessories

Recommended lenses

- LTC 3764/20 Varifocal Lens
  - 1/2-inch, 4 -12 mm, DC-iris, C-mount, F/1.2-360, 4 pin
- LTC 3774/30 Varifocal Lens
  - 1/2-inch, 10 - 40 mm, DC-iris, C-mount, F/1.4-360, 4-pin
- LTC 3783/50 Zoom Lens
  - 1/2-inch, 8.5 - 85 mm, video-iris, C-mount F/1.6-360, 4-pin
- LTC 3793/50 Zoom Lens
  - 1/2-inch, 8 - 144 mm, video-iris, C-mount, F/1.6-360, 4-pin
- LTC 3664/40 Varifocal Lens
  - 1/3-inch, 2.8 - 11 mm, DC-iris, CS-mount F/1.4-360, 4-pin
- LTC 3664/30 Varifocal Lens
  - 1/3-inch, 3.0 - 8 mm, DC-iris, CS-mount F/1.0-360, 4-pin

Power transformers

- TC 120PS Power Supply Unit
  - 110-120 VAC/15 VDC, 50/60 Hz, 300mA
- TC 220PS Power Supply Unit
  - 230 VAC/15 VDC, 50 Hz, 10 VA

13 Glossary

Brief explanations of some of the terms and abbreviations found in this user guide are given below.

10/100 Base-T	IEEE 802.3 specification for 10 or 100 MBit/s Ethernet
ARP	Address Resolution Protocol: a protocol for mapping MAC and IP addresses
Baud	Unit of measure for the speed of data transmission
Bit/s	Bits per second, the actual data rate
CIF	Common Intermediate Format, video format with 352 x 288/240 pixels
DNS	Domain Name Service
FTP	File Transfer Protocol
Full duplex	Simultaneous data transmission in both directions (sending and receiving)
Gateway	Access point to another LAN (subnet)
GOP	Group of pictures
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ID	Identification: a machine-readable character sequence
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
Internet Protocol	The main protocol used on the Internet, normally in conjunction with the Transfer Control Protocol (TCP): TCP/IP
IP	*See* Internet Protocol
IP address	A 4-byte number uniquely defining each device on the Internet. It is usually written in dotted decimal notation with full stops separating the bytes, for example "209.130.2.193".
ISDN	Integrated Services Digital Network
JPEG	An encoding process for still images (Joint Photographic Experts Group)
kBit/s	Kilobits per second, the actual data rate

LAN	*See* Local area network
Local area network	A communications network serving users within a limited geographical area, such as a building or a university campus. It is controlled by a network operating system and uses a transfer protocol.
MAC	Media Access Control
MPEG-4	Further development of MPEG-2, designed for transmission of audiovisual data at very low transfer rates (for example via the Internet).
Net mask	A mask that explains which part of an IP address is the network address and which part comprises the host address. It is usually written in dotted decimal notation with full stops separating the bytes, for example "255.255.255.192".
Parameters	Values used for configuration
QCIF	Quarter CIF, a video format with 176 × 144/120 pixels
RFC 868	A protocol for synchronizing computer clocks over the Internet
RS232/RS422/RS485	Standards for serial data transmission
RTP	Realtime Transport Protocol; A transmission protocol for real-time video and audio
Subnet mask	*See* Net mask
TCP	Transfer Control Protocol
Telnet	Login protocol with which users can log on to a remote computer (host) on the Internet
TTL	Time-To-Live; life cycle of a data packet in station transfers
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
WAN	*See* wide area network
Wide area network	A long distance link used to extend or connect remotely located local area networks

Bosch Sicherheitssysteme GmbH
Ludwig-Bölkow-Allee
85521 Ottobrunn
Germany
www.bosch-sicherheitssysteme.de

Bosch Security Systems B.V.
P.O. Box 80002
5600 JB Eindhoven
The Netherlands
www.boschsecuritysystems.com

9922 141 0xxxx 06-15
© 2006 Bosch Security Systems B.V.
Subject to change. Printed in Portugal.

BOSCH